2/2018

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

41. Jahrgang
ISSN 0137-7767
12,00 Euro



■ Die Umsetzung der DSGVO in Deutschland ■ Das neue Recht auf Datenübertragbarkeit aus Sicht der Betroffenen ■ Vereine unter der DSGVO ■ Der Betriebsrat als datenschutzrechtlicher „Verantwortlicher“ im Sinne der DSGVO ■ 40 Jahre DANA – Rückblick eines nicht völlig Unbeteiligten ■ BigBrother-Awards 2018 ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Mittwoch, 01. August 2018
Redaktionsschluss DANA 3/2018

Sonntag, 09. September 2018
Vorstandssitzung der DVD in Kiel
Interessenten melden sich bitte in der Geschäftsstelle der DVD an.

Montag, 10. September 2018
Sommerakademie des ULD Schleswig-Holstein
https://datenschutzzentrum.de/sommerakademie/2018/

Samstag, 20. Oktober 2018
DVD-Vorstandssitzung
Bonn

Sonntag, 21. Oktober 2018
DVD-Mitgliederversammlung
Bonn

Donnerstag, 01. November 2018
Redaktionsschluss DANA 4/2018

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
41. Jahrgang, Heft 2

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Frank Spaeing
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, Adobestock, pixelio, digitalcourage, iStock,

Editorial

Der 25.05.2018 liegt hinter uns. Wir leben im Zeitalter der Datenschutzgrundverordnung. Und jetzt?

In den letzten Wochen (vor und auch seit dem 25.05.2018) hat sich Hektik breit gemacht in Deutschland, in Europa und in der Welt. Facebook hat kurz vor der Anwendbarkeit der Datenschutzgrundverordnung (DSGVO) noch schnell ca. 1,5 Milliarden Nutzerkonten aus irischen Rechenzentren in andere Rechenzentren weltweit verschoben, um diese in Zukunft nicht nach der DSGVO verarbeiten zu müssen.

Webseitenbetreiber haben aus Angst vor Abmahnungen ihre Webseiten zum 25.05.2018 abgeschaltet. Viele Menschen in Deutschland haben sich über Unmengen an Mails in ihren Posteingängen gewundert, die sie darüber informierten, dass sie ohne Einwilligung leider nicht mehr Mails vom Absender bekommen könnten.

Datenschutzbeauftragte scheinen gefühlt zu einer extrem raren Spezies geworden zu sein, denn fast überall wird geklagt, dass der Markt der Datenschutzbeauftragten und -berater abgegrast ist und dass auch niemand mehr für Datenschutz qualifizierte Mitarbeiter auf dem freien Arbeitsmarkt findet.

Nun stellt sich also die Frage „Und jetzt?“, wie geht es weiter im Datenschutz?

In der vorliegenden DANA-Ausgabe widmen sich unsere Autoren Themen, die alle in diese Zeit des Umbruchs passen und sich an dieser Frage abarbeiten – entweder weil sie den aktuellen Zustand beschreiben (Thilo Weichert - Die Umsetzung der DSGVO in Deutschland), weil sie neue Thematiken erklären (Anne Riechert - Das neue Recht auf Datenübertragbarkeit aus Sicht der Betroffenen), weil sie alte Fragestellungen nach dem neuen Recht betrachten (Robert Zieske - Der Betriebsrat als datenschutzrechtlicher „Verantwortlicher“ im Sinne der DSGVO) oder weil sie schlicht und ergreifend Hinweise zur Umsetzung geben wollen (Philipp Schmidtke - Vereine unter der DSGVO).

Außerdem wird vom BigBrotherAward 2018 berichtet, das EuGH-Urteil zu Facebook-Fanpages kommentiert und die aktuelle Presseerklärung der DVD zur gescheiterten Wahl des neuen Landesdatenschutzbeauftragten in Sachsen-Anhalt abgedruckt.

Abgeschlossen wird das vorliegende Heft wie üblich mit Datenschutz- und Techniknachrichten, aktueller Rechtsprechung und Buchbesprechungen.

Und alle behandelten Themen zeigen uns, dass der Umbruch noch lange nicht beendet ist, dass die unruhigen Zeiten uns wohl noch einige Zeit begleiten werden.

Ich wünsche Ihnen eine interessante Lektüre für die Sommertage.

Frank Spaeing

Autorinnen und Autoren dieser Ausgabe:

Heinz Alenfelder
Vorstandsmitglied in der DVD,
alenfelder@datenschutzverein.de, Köln

Prof. Dr. Anne Riechert
Stiftung Datenschutz, a.riechert@stiftungdatenschutz.org

Klaus-Jürgen Roth
dvd@datenschutzverein.de

Philipp Schmidtke
Ass.Jur., Datenschutzberater der ds² Unternehmensberatung GmbH & Co. KG,
philipp.schmidtke@ds-quadrat.de

Dr. Thilo Weichert
Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Robert Zieske
Datenschutzjurist und Referent bei der Deutschen Kreditbank AG,
robert.zieske@gmx.de

Thilo Weichert

Die Umsetzung der DSGVO in Deutschland

Die Umsetzung europäischen Rechts in den einzelnen EU-Mitgliedstaaten wird bestimmt durch die jeweilige nationale Geschichte vor dem Entstehen der europäischen Rechtsnormen, durch regionale Einflussnahmen auf die EU-Gesetzgebung, durch innerstaatliche Debatten sowie die administrative und gerichtliche Anwendung der Regelungen. Bei der Europäischen Datenschutz-Grundverordnung (DSGVO) kommt als weiterer Aspekt das Erlassen flankierender (umsetzender) nationaler Gesetze hinzu, für die es angesichts der vielen Spezifizierungs- bzw. Öffnungsklauseln in der DSGVO einen großen Spielraum gibt.

1 Vorgeschichte

Die deutsche Geschichte des Datenschutzes ist schillernd und geht weit zurück. Sie beeinflusste die Geschichte des Datenschutzes generell. Wesentliche *Impulse* für den Datenschutz in Europa und global wurden in Deutschland durch Bundesländer gesetzt.

Die Vorgeschichte beginnt nicht erst im Jahr 1970, als in Hessen das weltweit erste moderne Datenschutzgesetz erlassen wurde[1], sondern erheblich früher. Eine Quelle liegt in der juristischen *Entwicklung eines allgemeinen Persönlichkeitsrechts* durch die Rechtsprechung des Reichsgerichts und später des Bundesgerichtshofes (BGH) in Form von speziellen Ausprägungen und Differenzierungen. So wurde das Recht am eigenen Bild im Jahr 1907 im Kunsturhebergesetz normiert. Es folgte das Recht am gesprochenen Wort. Im berühmten Herrenreiterurteil des BGH aus dem Jahr 1958[2] entwickelte das höchste deutsche Zivilgericht jenseits der klassischen Einteilung von öffentlicher, sozialer und intimer Sphäre aus dem Persönlichkeitsrecht einen Anspruch auf Selbstvermarktung. Damit wurden rechtliche Grundlagen geschaffen, die sich vom üblichen Privatsphärenschutz absetzen, wie er z. B. in Art. 12 der Allgemeinen Erklärung der Menschenrechte vom 10.12.1948 definiert wird mit dem Schutz des Menschen vor „willkürlichen Eingriffen in sein Privatleben, seine Familie, sein Heim oder seinen Briefwechsel". Das Konzept des Schutzes der Privatheit bzw. von Privacy, wie es in der Menschenrechtserklärung normiert ist, ist bis heute z. B. in den USA vorherrschend, auch wenn es – als ausschließliches Schutzkonzept – spätestens seit der informationstechnischen Entwicklung in den 70er Jahren des letzten Jahrhundert nicht mehr passt und immer weniger zeitgemäß wird.

Es ist interessant, dass in den USA eher als in Europa, mit dem Aufsatz von Samuel D. Warren und Louis D. Brandeis zum „Right to Privacy"[3], ein modernes Verständnis ausgearbeitet und insbesondere von Alan F. Westin in den 60er Jahren[4] weiterentwickelt wurde. Dieser Ansatz der „information privacy" gegen „data surveillance", der sich in den USA aber bis heute nicht durchsetzen konnte, wurde vom deutschen Recht teilweise rezipiert. Prägend für die Weiterentwicklung des allgemeinen Persönlichkeitsrechts zu einem Recht auf Datenschutz war in Deutschland in den 60er Jahren zudem die kritische Aufarbeitung des Nationalsozialismus, der Informationstechnik nutzte, um ethnische, kulturelle und politische Minderheiten zu erfassen, zu unterdrücken, zu verfolgen und zu vernichten. Vor diesem historischen Hintergrund entstand 1971 das Gutachten „Grundfragen des Datenschutzes" von Steinmüller und anderen, das die Basis für die deutsche Gesetzgebung legte. Diese nahm als Ausgangspunkt nicht die Privatsphäre, sondern das personenbezogene Datum.[5]

Die weitere *deutsche Entwicklung* wurde vielfach beschrieben und kann weitgehend als bekannt vorausgesetzt werden.[6] Meilensteine waren dabei das Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983[7] sowie die Etablierung der Datenschutzgesetze in den Ländern und auf Bundesebene, nach der Vereinigung 1990 auch in den neuen Bundesländern. Erneut war die Erfahrung mit einem totalitären Gesellschaftsmodell, das der DDR, in der staatliche Überwachung eine zentrale Rolle spielte, förderlich für die Adaption eines demokratisch und freiheitlich verstandenen Datenschutzes.

Die Erarbeitung der *europäischen Datenschutzrichtlinie*, die 1996 in Kraft trat,[8] war stark von der deutschen Gesetzgebung geprägt. Es flossen zudem Mechanismen aus anderen Staaten ein, etwa die Idee der Selbstregulierung durch Verhaltensregeln oder das Verbot automatisierter Einzelentscheidungen. Schon bei der Umsetzung der EG-Datenschutzrichtlinie von 1996 zeigte sich, dass die nationale Politik der Bundesregierung nicht danach strebte, die Richtlinie optimal umzusetzen. Erst drei Jahre nach der vorgegebenen Frist, nämlich 2001, wurde ein Bundesdatenschutzgesetz verabschiedet, das wenig innovativ und eher bürokratisch war.[9]

Zuvor waren es wieder die *Bundesländer*, die inhaltlich die Richtung vorgaben. In den ersten Jahren der deutschen Datenschutzgesetzgebung war Hessen unter dem Einfluss von Spiros Simitis wegweisend und inspirierend. Nach der EG-Richtlinie 1995 war es Schleswig-Holstein, das unter dem Einfluss von Helmut Bäumler im Jahr 2000 innovative und moderne Elemente ins Datenschutzrecht einführte: Das dortige Landesdatenschutzgesetz enthielt einen umfassenden Verarbeitungsbegriff, eine Regelung zu Datenvermeidung und Datensparsamkeit, sah Gütesiegel- und Auditverfahren und ein strukturiertes Verfahren bei der Einführung neuer Informationstechnik (IT) mit Dokumentation, Test und Freigabe vor, regelte den technischen Datenschutz technikneutral über Schutzziele, benannte explizit spezielle Sicherungsmaßnahmen wie z. B. die Verschlüsselung, normierte gemeinsame Verfahren, mobile Systeme und die Internetveröffentlichung, privi-

legierte die pseudonyme Datenverarbeitung und ergänzte das Aufsichtsregime um Service-, Beratungs- und Zertifizierungsfunktionen.[10] In der Praxis kamen Forschungsaktivitäten der Aufsichtsbehörde hinzu. Vieles von dem, was 2000 in Schleswig-Holstein Gesetz und Praxis wurde, war damals weltweit einzigartig und findet sich heute in der DSGVO wieder. Keines dieser Instrumente wurde von der Bundespolitik bei der Ausarbeitung der DSGVO offensiv gefördert, Einiges aber zumindest aufgegriffen (z. B. Datensparsamkeit, Audits, Definition der Pseudonymisierung).

Der bisher letzte *innovative Impuls*, der aus Deutschland hinsichtlich des digitalen Grundrechtsschutzes kam, stammte nicht aus der Politik, sondern vom Bundesverfassungsgericht, das 2008 analog zum Schutz der räumlichen Privatsphäre in Art. 13 GG oder der sozialen Privatsphäre der Familie in Art. 6 GG einen besonders schützenswerten Bereich digitaler Privatsphäre in Form des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schuf.[11] Positive gesetzgeberische Konsequenzen wurden aus diesem Urteil bis heute nicht gezogen.

Bezeichnend ist, dass auch in anderen Bereichen des digitalen Grundrechtsschutzes nicht der Bundes-, sondern die Landesgesetzgeber innovationsfördernd waren bzw. sind. So ist in Deutschland bisher nur in Brandenburg ein allgemeines *Recht auf Informationszugang* verfassungsrechtlich verankert.[12] Auch das deutsche Bundesverfassungsgericht verweigert sich hier der grundgesetzlichen Anerkennung neuer Informationsrechte, die für eine demokratische Informationsgesellschaft essenziell sind. In diesem Fall waren es die Bundesländer Brandenburg (1998), Berlin (1999), Schleswig-Holstein (2000) und Nordrhein-Westfalen (2001), bevor auch der Bund zumindest auf einfachgesetzlicher Ebene einen Anspruch auf Zugang zu hoheitlichen Informationen normierte. Vorbilder waren politisch insofern die USA und die skandinavischen Länder[13]; in der Rechtsprechung sind dies der Europäische Gerichtshof in Luxemburg und der Europäische Gerichtshof für Menschenrechte in Straßburg.

2 Die Verabschiedung der DSGVO

Mit dem Beginn der Diskussion über die DSGVO 2012 verlagerte sich der Schwerpunkt der Datenschutzdiskussion vollständig nach Brüssel bzw. nach *Europa*. Insbesondere die zuständige Kommissarin Viviane Reding und der Berichterstatter im EU-Parlament Jan-Philipp Albrecht sorgten dafür, dass Sabotageversuche von Gegnern digitaler Grundrechte abgewehrt und eine fortschrittliche Gesetzgebung vorangetrieben wurden.

Die *deutsche Politik* stellte sich an die Spitze der Saboteure. Durch ihre innerhalb und außerhalb der EU-Institutionen vorgetragenen Bedenken und die politische Querschüsse war insbesondere die Bundesregierung dafür verantwortlich, dass sich die Verabschiedung der DSGVO verzögerte. Inhaltliche Versuche der Verwässerung wurden von den EU-Gremien zurückgewiesen. Es wurde versucht, anstelle einer direkt anwendbaren Verordnung lediglich eine einen allgemeinen Rahmen festlegende Richtlinie durchzusetzen. Der Bundesrat demonstrierte mit einer Subsidiaritätsrüge sein provinzielles Verständnis vom Datenschutz. Der damalige Bundesinnenminister Hans-Peter Friedrich brachte anstelle der staatlichen Regulierung privatwirtschaftliche Selbstregulierung ins Gespräch. Sein Ministerium veranstaltete Symposien und Tagungen, in denen Wirtschaftsvertreter das Wort führten, die für den privaten Bereich die Abschaffung des Gesetzesvorbehalts forderten. Ironischerweise erfolgte dieser Widerstand gegen die DSGVO mit dem Verweis auf die angeblich so fortschrittliche deutsche Datenschutzgesetzgebung, die sich seit 2001 nur wenig weiterentwickelt und nicht modernisiert hatte. Noch Ende 2015, wenige Tage vor dem Abschluss des Trilogs zwischen Kommission, Parlament und Europäischem Rat, profilierte sich die Spitze der Bundesregierung mit Angela Merkel, Siegmar Gabriel und Alexander Dobrindt parteiübergreifend mit Angriffen auf die in der DSGVO vorgesehene Zweckbindung und das Prinzip der Datensparsamkeit. Beseelt von Eindrücken aus Pilgerfahrten ins Silicon Valley erklärten sie unisono, mit Zweckbindung und Datensparsamkeit würden die Entfaltung der IT-Wirtschaft in Europa und die Entwicklung des segensreichen Big Data behindert. Um das „Öl des 21. Jahrhunderts“, personenbezogene Daten, nutzbar zu machen, müsse die Zweckbindung aufgeweicht und „Datenreichtum“ praktiziert werden.[14]

Von derartigen Angriffen relativ unbeeindruckt einigten sich die europäischen Institutionen nicht nur auf ein Präzisierung der Datensparsamkeit und der Zweckbindung, sondern auf weitere *zeitgemäße Instrumente des digitalen Grundrechtsschutzes* in einer globalisierten Informationsgesellschaft: harmonisierte verbindliche Regelungen, Marktortprinzip, One-Stop-Shop für Unternehmen und Betroffene, verbesserte Betroffenentransparenz, „Privacy by Default“ und „Privacy by Design“, generelle Anwendbarkeit der Datenschutz-Folgenabschätzung, rechtssicherere Drittlands-Datentransfers, verbesserte Beschwerde- und Rechtsschutzmöglichkeiten, wirksame Sanktionen.

3 Wider eine unabhängige und wirksame Datenschutzkontrolle

Man sollte erwarten, dass die deutsche Politik, die sich gegenüber dem europäischen Gesetzgeber nicht durchsetzen konnte, nun den von der EU gesetzten rechtlichen Rahmen akzeptieren und umsetzen würde. Doch erleben wir bei der Umsetzung der DSGVO wie auch der zeitgleich verabschiedeten Datenschutzrichtlinie für Polizei und Justiz eher das Gegenteil: Was in Brüssel erreicht wurde, versuchen Berlin und einige Landeshauptstädte wieder zurückzuschrauben. Einfallstore hierfür sind die vielen *Öffnungsklauseln*. Die von der Bundespolitik vorgegebene Strategie ist offensichtlich: Wenn schon viele materielle Regelungen von Europa festgelegt sind, so kann deren Anwendung prozedural beschränkt werden. Die Politik beschreitet dabei nicht nur den Weg über die Haushalte, indem die Aufsichtsbehörden so schwach ausgestattet werden, dass sie mangels Personal und Ressourcen den Anforderungen zur Gesetzesumsetzung schlicht nicht genügen können. Diese Strategie wird vor vielen Bundesländern mit erschreckender Konsequenz verfolgt. Verblüffend ist, dass lammfromme Beauftragte

wie z. B. auf Bundesebene für ihre Zahnlosigkeit zumindest mit einem gewissen Ressourcenzuwachs belohnt wurden. Die Aufsichtsbehörde in Hamburg, zuständig in Deutschland für Google, Facebook und viele weitere große Unternehmen, soll ihre Aufgabe künftig mit insgesamt 25 Stellen stemmen – ein absurdes Ansinnen![15]

Ungenügende Ausstattung scheint aber als Rückversicherung nicht zu genügen, um den Vollzug der DSGVO zu behindern. Dank der Lobbyarbeit insbesondere von Anwaltsverbänden wurde die gesamte *Datenschutzprüfung im Bereich von Berufsgeheimnissen* in § 29 Abs. 3 BDSG so reguliert, dass umfassende Kontrollen unmöglich gemacht werden können. Entgegen der deutschen Gesetzeslage wurde der Staatsanwaltschaft justizielle Unabhängigkeit zugesprochen und diese so von Aufsichtskontrollen freigestellt.[16] Dem Landesgesetzgeber in Niedersachsen genügte selbst dies nicht. Er erklärte gleich das gesamte strafrechtliche Ermittlungsverfahren einschließlich der polizeilichen Datenerhebung, Speicherung und Auswertung für kontrollfrei.[17] Dass es sich bei der Verarbeitung von Berufsgeheimnissen sowie bei strafrechtlichen Ermittlungen um persönlichkeitsrechtlich besonders intensive Eingriffe handelt und insofern das BVerfG eine besonders intensive Prüfung einforderte[18], ließ die jeweiligen Gesetzgeber kalt. Diese nahmen damit sehenden Auges einen Verstoß gegen deutsches Verfassungsrecht und zugleich auch einen Verstoß gegen die bedingungslos formulierte unabhängige Kontrollzusicherung in Art. 8 Abs. 3 Grundrechte-Charta in Kauf.

Auch gegen die Unabhängigkeit der Datenschutzaufsicht fand der deutsche Gesetzgeber wirksame Vorkehrungen. So ignorieren Bund wie Länder das europarechtliche Erfordernis eines *transparenten Bestellungsverfahrens*. Die bisherigen Geheimprozesse bei der Auswahl der Behördenleitungen werden fortgeschrieben. Die Notwendigkeit einer Ausschreibung sowie einer öffentliche Diskussion über die Auswahl ist nirgends vorgesehen. Die Besetzung der Stellen war schon bisher oft davon bestimmt, verdiente Politiker zu versorgen und auf Kompetenz und Erfahrung der Kandidaten zu verzichten. Dies ist zwar künftig im EU-Recht ausdrücklich verboten. Ob dies auch umgesetzt wird, muss sich zeigen.[19]

Ein Angriff auf die Unabhängigkeit enthält auch die Repräsentanz Deutschlands im europaweit zentralen Datenschutzgremium – dem *Europäischen Datenschutzausschuss* (EDSA). Während der Vorsitz bei der Bundesbeauftragten liegen soll, die nach deutschem föderalen Recht nur einen eingeschränkten Zuständigkeitsbereich hat und insbesondere nicht für die Aufsicht in der Privatwirtschaft zuständig ist, wird die Vertretung der Landesaufsicht im EDSA – unter Missachtung von deren Unabhängigkeit – politisch vom Bundesrat bestimmt.[20]

Der Angriff auf die föderale Struktur der unabhängigen Datenschutzaufsicht beschränkt sich nicht hierauf: Vielmehr wird zentralisiert, wo es nur geht: Schon in den Jahren 2011/2012 wurde die Aufsicht für wesentliche Sozialbereiche (Arbeitslosenverwaltung, Krankenkassen) von den Ländern auf den Bund übertragen.[21] Die nächste Kompetenzbeschneidung der Länderaufsicht erfolgte 2017 für die Finanzverwaltung. Derart stellt das Bundesfinanzministerium sicher, dass es sich nicht mehr mit missliebiger Kritik der Landesaufsicht an Datenschutzverstößen der Steuerbehörden, etwa durch die Verweigerung des Auskunftsrechtes, auseinandersetzen muss. Obwohl hier weitestgehend Landesbehörden tätig werden, wurde die Aufsicht einfach der Bundesbeauftragten zugeschlagen.[22]

Die Datenschutzkontrolle wird zudem durch die *Beschneidung der Abhilfebefugnisse* behindert, die – so das EU-Recht – wirksam sein müssten. Tatsächlich verzichtet das BDSG hierauf explizit im gesamten Telekommunikations- und Postbereich.[23] Statt den potenziell hohen Bußgeld-Sanktionen, wie sie in der DSGVO vorgesehen sind, soll hier als schärfstes Schwert weiterhin die zumeist völlig unwirksame förmliche Beanstandung zur Anwendung kommen. Dem folgend sehen die deutschen Datenschutzgesetze künftig auch keine wirksamen Sanktionen gegenüber öffentlichen Stellen vor. Es ist eine geradezu klassische Erfahrung der Datenschutzkontrolle im öffentlichen Bereich, dass die mit einer Beanstandung verknüpfte förmliche Feststellung der Rechtswidrigkeit einer Datenverarbeitung nicht zu deren Beendigung führt. Gerade bei der schon angesprochenen Finanzverwaltung und bei den Strafverfolgungs- und sog. Sicherheitsbehörden werden Datenschutzverstöße regelmäßig von der Fach-, Dienst- und Rechtsaufsicht gedeckt. Diese erweist sich oft als besonders unsensibel in Datenschutzfragen und als unrechtstreu. Es scheint erklärter politischer Wille zu sein, dass sich hieran nichts ändert.

Es ist kein Trost, dass es *andere EU-Staaten* Deutschland nachmachen oder gar die Falsch- oder Nichtumsetzen des EU-Rechts noch toppen, allen voran Österreich, das mit seiner ÖVP-FPÖ-Mehrheit aus dem Datenschutzrecht einen zahnlosen Tiger zu machen versucht, der nur wenig brüllen und fast gar nicht mehr beißen darf.[24]

4 Wider die Verständlichkeit

Man kann die DSGVO sicherlich dafür kritisieren, dass sie oft vage formuliert ist. Auch sind manche Begrifflichkeiten wenig überzeugend gewählt bzw. ins Deutsche übersetzt. Doch kann man der DSGVO nicht den Vorwurf machen, sie sei *unsystematisch aufgebaut und schwer verständlich*. Dieses schon bisher bestehende Defizit des deutschen Datenschutzrechts wird bei der Umsetzung der DSGVO fortgeführt, ja noch gesteigert.

Die deutschen Gesetzgeber haben es sich fast durchgängig zur Aufgabe gemacht, das nationale Recht so umständlich zu formulieren, dass es von normalen Menschen überhaupt nicht, und von Fachleuten nur nach einem umfassenden Studium verstanden und ausgelegt werden kann. Es ist geradezu absurd, dass das deutsche Recht praktisch durchgängig die DSGVO nicht beim Namen nennt, sondern mit der Bezeichnung „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016; L 314 vom 22.11.2016, S. 72) in der jeweils geltenden Fassung" beschreibt[25] oder mit dem nicht weniger allgemein verständlichen „Kürzel" *„Verordnung (EU) 2016/679"*.[26]

Dass es anders geht zeigte der bayerische Gesetzgeber, der einmal für die „DSGVO" eine Quellenangabe vornimmt und diese Bezeichnung danach so (ohne Bindestrich!) verwendet.[27] Auch die Verwendung des ausgeschriebenen Namens „Datenschutz-Grundverordnung" ist bürgerfreundlicher und verständlicher, als das, was die Ministerialbürokratie den Gesetzgebern regelmäßig vorgegeben hat bzw. vorgibt.

Die Anwendbarkeit des Datenschutzrechts wird weiter dadurch erschwert, dass nicht versucht wurde, die Umsetzung der DSGVO-Regelungen direkt im bereichsspezifischen Recht vorzunehmen. Dies hat zur Folge, das oft Regeln aus drei Ebenen anzuwenden sind: 1. DSGVO, 2. umsetzende allgemeine nationale oder Landesnormen, 3. bereichsspezifisches Recht. Das BDSG bzw. die Landesdatenschutzgesetze (LDSG) werden zu einer Art *Scharnierrecht*, in dem oft, aber nicht immer, nur die Öffnungsklauseln der DSGVO paraphrasiert werden. Das dadurch verursachte Regelungschaos ist besonders groß, weil in Deutschland die Öffnungsklauseln extensiv und oft über den zulässigen Rahmen hinaus in Anspruch genommen wurden. In der DSGVO angelegte Abwägungsregeln sind als solche im nationalen Recht oft nicht zu erkennen, so dass zusätzlich zur nationalen Norm auf die DSGVO-Grundnorm zurückgegriffen werden muss. Insbesondere bei den durch die DSGVO grds. zugelassenen Einschränkungen der Betroffenenrechte werden äußerst unbestimmte Formulierungen verwendet, so dass die Rechtsanwendenden keine klaren Vorgaben erkennen können.

5 Die Praxis des Datenschutzes

Es ist – ohne dass diese Feststellung von den *Datenschutzbehörden* als Kritik an der eigenen Tätigkeit wahrgenommen werden muss – offensichtlich, dass wir in Deutschland ein gewaltiges Vollzugsdefizit beim Datenschutz hatten und weiterhin haben. Dies hat viele Gründe. Einer ist die teilweise katastrophale Ausstattung der Aufsichtsbehörden.[28] Ein weiterer Grund ist die bisher maximale Sanktionshöhe von 300.000 €, die bei rechtswidrig agierenden Globalkonzernen wie Google, Microsoft oder Facebook bisher nur ein müdes Lächeln auslöste. Ein weiterer Grund war, dass, wie schon dargestellt, der Datenschutz in der offiziellen Politik keine oder kaum eine Lobby hatte, geschweige denn auf Verständnis oder gar auf Engagement stieß und weiterhin stößt.[29] Selbst eine sich als digitale Bürgerrechtspartei gerierende Partei wie die FDP konnte im Bundestagswahlkampf 2017 ungestraft von ihren Wählern bundesweit plakatieren „Digital first – Bedenken second",[30] wobei mit Bedenken nicht zuletzt der Datenschutz gemeint war.

Im zeitlichen Vorlauf zur direkten Anwendbarkeit der DSGVO haben wir ein erstaunliches Phänomen erlebt: Rechtsanwälte, Unternehmensberater und professionelle Datenschützer mussten vor dem 25.05.2018 Überstunden schieben. Zwar war seit 2 Jahren bekannt, welche Datenschutzregeln künftig gelten. Doch bewusst wurde es vielen Behörden und Privatunternehmen erst weniger als ein halbes Jahr vor dem Termin. Einen wesentlichen Beitrag zur großen Datenschutznachfrage leisteten Geschäftemacher, die mit der starken *Sanktions- und Abmahnmöglichkeiten* dafür warben, die Aufgabe des Datenschutzes auf sich outzusourcen und damit oft für überteuertes Geld in wenig kompetente Hände zu übertragen.[31] Dabei handelte es sich nicht um eine Aufklärungs-, Werbe- oder Sympathiekampagne, sondern um ein *Drohszenario*, das nicht nur völlig überzogen war und ist, sondern auch oft mit falschen Fakten argumentierte. So sehr dies zu kritisieren ist, bewirkt hat dies, dass sich viele Unternehmen erstmals überhaupt mit Datenschutz beschäftigt haben. Wer sich bisher an das Recht gehalten hat, muss auch in Zukunft wenig befürchten: Aufsichtsbehörden sind nicht nur aus Kapazitätsgründen dem Verhältnismäßigkeitsgrundsatz verpflichtet. Als zusätzliche von Abmahnvereinen feststellbare Pflichtverletzung kommt bei Internetpräsenz allenfalls die Informationspflicht nach Art. 12 ff. DSGVO in Betracht, die einzuhalten kein Hexenwerk darstellt.

Es ist nun leider so, dass es tatsächlich bei vielen der Drohung bedurfte, dass der Datenschutz ernst genommen wird. Dieser Ernst könnte schnell verfliegen, wenn sich die Aufsichtsbehörden nicht vom ersten Tag an auf die neue Rechtslage umstellen. Dies ist – insbesondere aus Kapazitätsgründen – eine *Herkulesaufgabe*, zumal die politische Rückenstärkung weiterhin weitgehend fehlt. Da muss der behördliche Datenschutz jetzt durch, will er sich nicht auf längere Zeit ganz verabschieden. Zur Herkulesaufgabe gehört es, zeitnah auf Anfragen und Beschwerden zu reagieren. Es geht nicht an, dass ich z. B. für eine gut begründete juristisch ausgearbeitete Beschwerde gegen ein in Deutschland agierendes US-amerikanisches Petitionsportal trotz mehrfacher Anfragen außer einem Zwischenbescheid bis heute keine Antwort bekommen habe.[32] Wenn das Personal für die Bearbeitung fehlt, so muss es von den Behörden offensiv eingefordert werden.

Ein Lichtblick für den Datenschutz ist schon seit einigen Jahren, in jedem Fall seit der Zulassung der *Verbandsklage bei Datenschutzverstößen*, der Verbraucherschutz.[33] Dieser betätigt sich nicht als Konkurrenz, sondern als natürliche Ergänzung zu den Aufsichtsbehörden. Die DSGVO bestärkt in Art. 80 diese Entwicklung. Würden echte Sammelklagen zugelassen, und nicht nur, wie in Deutschland geplant, sog. Musterfeststellungsklagen, so wäre der Effekt des Verbraucherschutzes sicher noch erheblich größer.

Ein weiterer Lichtblick sind im Bereich des Beschäftigtendatenschutzes in jüngerer Zeit einige *Betriebsräte*.[34] Diese haben die Möglichkeit und das Recht, durch Kollektivvereinbarungen – nun im Rahmen des Art. 88 DSGVO – gemeinsam mit den Arbeitgebern rechtssetzend tätig zu werden. Sie stoßen zwar hinsichtlich des informationstechnischen und des rechtlichen Know-hows allzu oft an Grenzen. Insofern muss und kann mit Beratung gegengesteuert werden. Mangelnde Kooperationsbereitschaft der Arbeitgeber stößt künftig auf ein umfängliches Abhilfeinstrumentarium. Da inzwischen selbst die Gewerkschaften das Thema entdeckt haben, wenngleich dort das Bewusstsein für die Problematik entwicklungsfähig ist, gibt es Anlass zum Optimismus. Dass wir auch 35 Jahre nach dem Volkszählungsurteil immer noch kein Beschäftigtendatenschutzgesetz haben[35], lag bisher nicht nur am Unwillen der Politik und der Arbeitgeberseite, sondern auch am feh-

lenden Bewusstsein und Druck seitens der Gewerkschaften.

So sehr sich die DSGVO aktuellen Herausforderungen bei der Umsetzung stellen muss, so gewaltig ist das in ihr steckende Potenzial. Dabei handelt es sich letztlich um das *globale Gegenmodell* zur den totalitären und autoritären Regulierungen in Russland oder in China sowie zum ökonomisch motivierten US-amerikanischen Regulierungsverzicht. Ein Gegenmodell ist die DSGVO dabei nicht nur als innergesellschaftliche Alternative zum vorherrschenden System, etwa für die (außerparlamentarische) Opposition in den USA. Es hat auch hohe Attraktivität für Schwellenstaaten, die sich den Hegemonialbestrebungen etwa von China oder den USA bei der Digitalisierung nicht unterordnen wollen.

Das BVerfG hat mit seiner Schrittmacherfunktion für den Datenschutz mit dem EuGH Unterstützung erhalten. Der EuGH hat die Möglichkeit, über den Rahmen nationaler Rechtsanwendung hinaus europaweit einheitliche Auslegungen vorzugeben. Angesichts des Umstands, dass von der deutschen Politik auf Bundes- und Landesebene keine Impulse zu erwarten sind, sind Impulse aus der *Rechtsprechung* umso wichtiger. Bei aller Kongruenz zwischen nationaler und europäischer Rechtsprechung im Bereich des Datenschutzes ist mit Aufmerksamkeit zu verfolgen, wie sich die Gerichtsentscheidungen in neuen Bereichen des digitalen Grundrechtsschutzes fortentwickeln. Hinsichtlich Transparenzansprüchen waren der EuGH sowie der Europäischen Gerichtshof für Menschenrechte erheblich fortschrittlicher als das BVerfG.

6 Verfassungsrechtliche Weiterentwicklungen

Die Beschränkung des Datenschutzes auf eine eng verstandene „informationelle Selbstbestimmung“ als subjektives Individualrecht[36] birgt in der Verwaltungspraxis Anwendungsrisiken: Schon früh war im Hessischen Datenschutzrecht anerkannt, dass es Aufgabe des Datenschutzes ist, „das auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Gefüge des Staates, insbesondere der Verfassungsorgane des Landes und der Organe der kommunalen Selbstverwaltung untereinander und zueinander, vor einer Gefährdung infolge der automatisierten Datenverarbeitung zu bewahren“.[37] In Frage stand das Informationsgleichgewicht zwischen Regierung und Parlament.[38] Das BVerfG hat in seinem Volkszählungsurteil zudem herausgestellt, dass Datenschutz „eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten *freiheitlichen demokratischen Gemeinwesens* ist“.[39] Direkte gesetzgeberische Konsequenzen sind aber aus dieser Erkenntnis bisher nicht gezogen worden.

Der rechtliche Ansatz der DSGVO ist in Art. 1 Abs. 1 erheblich weiter, indem er als Schutzzweck generell *„die Grundrechte und Grundfreiheiten natürlicher Personen“* nennt. Davon erfasst sind also auch der Schutz des Telekommunikationsgeheimnisses (Art. 7 GRCh), vor Diskriminierung (Art. 21 GRCh) und der Meinungs- und Informationsfreiheit (Art. 11 GRCh), das Recht auf Zugang zu Dokumenten (Art. 42 GRCh) sowie auch die Schutzrechte für Arbeitnehmer oder Verbraucher (Art. 27 ff., 38 GRCh).[40] Die unabhängigen Aufsichtsbehörden dürfen sich also nicht auf ein enges Verständnis beschränken, sondern müssen bei ihrer Aufgabenbeschreibung einem umfassenden Grundrechtsansatz folgen, der auch gesellschaftliche Funktionen wie Demokratie, Gewaltenteilung und Solidarität mit einschließt.

Letztlich führt die Digitalisierung nicht nur zu einer Gefährdung der bestehenden Grundrechte, sondern begründet den Bedarf der Entwicklung neuer, sich hieraus ergebender Instrumente. Mit einer *„Charta der Digitalen Grundrechte* der Europäischen Union“ wurde hierzu ein erster Diskussionsvorschlag vorgelegt.[41] Dabei geht es auch um einen sozial und freiheitlich verträglichen Einsatz von Algorithmen sowie von auf sog. künstlicher Intelligenz basierenden Verfahren. Für die Regulierung und Kontrolle derartiger Verfahren bedarf es dem Gemeinwohl verpflichteter, wirtschaftlich und politisch unabhängiger Instanzen mit rechtlicher wie technischer sowie sonstiger wissenschaftlicher Kompetenz und ausreichender Ausstattung. Für diese Funktion bietet sich der Ausbau der bestehenden Datenschutzaufsicht, die oft auch schon Aufgaben im Bereich der Informationsfreiheit wahrnimmt, an.

7 Praktischer Ausblick

Eine Bestandsaufnahme ist ohne einen Ausblick unvollständig. Die DSGVO enthält Potenziale, die noch nicht im Ansatz gehoben sind.

Dies gilt für die *Datenschutzzertifizierung*, die auch 18 Jahre, nachdem sie in Schleswig-Holstein eingeführt wurde, immer noch ein Schattendasein fristet. Ohne eine unabhängige, transparente und fachlich seriöse Zertifizierung werden künftig viele Datenschutzpflichten nicht verlässlich umgesetzt werden können.

Verhaltensregeln, also Normen der regulierten Selbstregulierung, haben bisher in der deutschen Datenschutzpraxis nur eine untergeordnete Rolle gespielt.[42] Dies kann und wird sich voraussichtlich ändern, da so nunmehr Entlastungen etwa für kleine und mittlere Unternehmen (KMU) erzielt und die Generalklauseln des Art. 6 DSGVO ausgefüllt werden können. Wirtschaftsverbände werden diese Möglichkeit voraussichtlich nutzen. Dadurch wird zugleich größtmögliche Sachnähe, Rechtssicherheit und Verbindlichkeit sowie kritische Kontrolle bewirkt.

Wurde Datenschutzrecht in den 70er Jahren als im öffentlichen Recht angesiedeltes Ordnungsrecht wahrgenommen, so emanzipierte sich der Datenschutz in den 90er Jahren im allgemeinen Zivilrecht und in den 00er Jahren speziell für den Verbraucher- und den Arbeitnehmerschutz. Seit Kurzem erobert der Datenschutz als Querschnittsmaterie immer mehr Rechtsgebiete. Besonders interessant sind die Querbezüge zum *Wettbewerbs-, Kartell- und Steuerrecht*. Durch die 9. GWB-Novelle[43] wird erstmals ausdrücklich die Datenkonzentration als mögliche Beeinträchtigung des Wettbewerbs anerkannt.

Die Weiterentwicklung des *Rechts der Digitalisierung* kann und darf mit der DSGVO nicht stehen bleiben. Die Hausaufgaben sind teilweise schon verteilt: Dies gilt für Europa, das derzeit die Datenschutzregeln für die EU-Institutionen und in der E-Privacy-Verordnung für den Bereich der Telekommunikation überarbeitet. Die EU kann aber nur im

Rahmen ihrer weiterhin beschränkten normativen Befugnisse tätig werden. Ihre Innovationskraft ist zudem durch den sehr weitgehenden Einigungszwang begrenzt. Hier sind eher nationale Initiativen nötig, die bei Bewährung von Brüssel übernommen werden können und sollten. Dabei stellt die föderale Struktur Deutschlands sowohl eine Chance wie auch ein Hindernis dar. Es ist unrealistisch, dass eine neue Föderalismusreform unter den Vorzeichen der Digitalisierung in Angriff genommen werden wird. Insofern sollten sich Bund und Länder auf das Instrument von Staatsverträgen besinnen, das sich im Medienbereich bewährt hat. Über *Bund-Länder-Staatsverträge* zu Digitalisierungsthemen, etwa für eine Forschungsinfrastruktur[44], können einheitliche Standards festgelegt werden, die regional wie national diskutiert werden müssen und dadurch letztlich ein hohes Akzeptanzpotenzial haben.

Ich wünsche mir für die Zukunft keine *Datenschutzskandale*. Wenn ich mir etwas wünschen dürfte, hielte ich eine massive Verletzung des Datenschutzes im Anwaltsbereich für besonders lehrreich. Es waren nämlich die Anwaltsverbände, die durch ihre Lobbypolitik gegenüber der Bundespolitik eine verfassungs- und europarechtswidrige Kontrolleinschränkung erreicht haben, die nicht nur dem Mandantengeheimnis, sondern letztlich der Anwaltschaft insgesamt schadet, ohne dass insofern bei den Anwaltsverbänden ein Erkenntnisprozess zu erkennen wäre.[45] Datenschutzskandale brachten in der Vergangenheit den Datenschutz voran. Die DSGVO in ihrer aktuellen Fassung wäre ohne die Snowden-Enthüllungen nicht möglich gewesen. Datenschutzskandale werden auch künftig passieren. Es wird darum gehen, hieraus die richtigen Schlussfolgerungen für den digitalen Grundrechtsschutz zu ziehen.

1 HDSG v. 30.09.1970, Hess. GVBl. 1970, 625.

2 BGH 14.02.1958 – I ZR 151/65, BGHZ 26, 349.

3 Warren/Brandeis, Harvard Law Review, Vol. IV Dec. 15, 1890 No. 5, Übersetzung in DuD 10/2012, 755 ff.

4 Westin, Privacy and Freedom, 1967.

5 Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider, Grundfragen des Datenschutzes, Juli 1971, BT-Drs. VI/3826.

6 Simitis in Simitis, BDSG, 8. Aufl. 2014, Einl. Rn. 1 ff.

7 BVerfG 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 419 ff.

8 Richtlinie 95/46/EG v. 24.10.1995, ABl. Nr. 281/31.

9 BDSG v. 22.05.2001, BGBl. I S. 904.

10 Landesdatenschutzgesetz SH, v. 09.02.2000, GS Schl.-H. II Gl.Nr. 204-4; ULD, Neues Datenschutzrecht in Schleswig-Holstein, 1. Aufl. 2000; Bäumler (Hrsg.), Der neue Datenschutz, 1998.

11 BVerfG U. v. 27.02.2008 – 1 BvR 370/07 u. 595/07, NJW 2008, 822.

12 Art. 21 Abs. 3, 4 BbgVerf.

13 Wegener, Der geheime Staat, 2006, S. 401 ff.

14 Weichert/Schuler, Datenschutz contra Wirtschaft und Big Data? www.netzwerk-datenschutzexpertise.de 31.12.2015.

15 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Tätigkeitsbericht Datenschutz 2016/2017, S. 18.

16 Weichert in Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, § 29 BDSG Rn. 24-29.

17 Kritisch zu den §§ 1 Abs. 2, 57 Abs. 3 NDSG Weichert, Stellungnahme, www.netzwerk-datenschutzexpertise.de 26.04.2018.

18 BVerfG U. v. U. v. 24.04.2013 – 1 BvR 1215/07, Rn. 215, NJW 2013, 1516.

19 Bernhardt/Ruhmann/Schuler/Weichert, Zum Auswahlprozess von Datenschutzbeauftragten als Leitung der Aufsichtsbehörden, www.netzwerk-datenschutzexpertise.de 03.02.2017.

20 Sommer in Däubler u. a. (Fn. 16) § 17 BDSG Rn. 4-7.

21 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Tätigkeitsbericht (TB) 2011, Kap. 4.5.1 (S. 47); ULD, TB 2013, Kap. 4.5.2 (S. 56).

22 Weichert in Däubler u. a. (Fn. 16) § 9 BDSG Rn. 7.

23 Weichert in Däubler u. a. (Fn. 16) § 16 Rn. 7 ff.

24 Krempl, Straflose Datenschutzverstöße: EU-Kommission will im Fall Österreich aktiv werden, www.heise.de 25.05.2018, vgl. DANA dieses Heft S. 113.

25 So z. B. § 31 Abs. 3b PatG.

26 So z. B. durchgängig im Sozialrecht, vgl. etwa § 67a Abs. 1 SGB X.

27 § 2 BayDSG.

28 Schulzki-Haddouti, Datensouveränität wiederherstellen! www.verdi.de 27.01.2017; zu den rechtlichen Grundlagen Weichert in Däubler u. a. (Fn. 16) Art. 52 Rn. 21-27; s. o. 3.

29 Netzwerk Datenschutzexpertise, Gabriel, Postmoderne und der Datenschutz, www.netzwerk-datenschutzexpertise.de 01.01.2018; Schuler/Weichert, Datenschutz contra Wirtschaft und Big Data? www.netzwerk-datenschutzexpertise.de 31.12.2015.

30 Kritisch Grau, Keine Bedenken und leider auch kein Denken, www.cicero.de 26.08.2017.

31 Tricarico, Die Panik, die wir riefen, taz 25.05.2018, 9.

32 Weichert, Datenschutzrechtliche Bewertung des Internet-Beteiligungsportals Change.org, www.netzwerk-datenschutzexpertise.de 15.11.2015.

33 Dazu rechtlich Weichert, Verbraucherverbandsklage bei Datenschutzverstößen, DANA 2017, 4 ff. = www.netzwerk-datenschutzexpertise.de 20.03.2017.

34 Eder in Wedde, Handbuch Datenschutz und Mitbestimmung, 2016, S. 185 ff.

35 Weichert/Schuler, Die EU-DSGVO und die Zukunft des Beschäftigtendatenschutzes, www.netzwerk-datenschutzexpertise.de 08.04.2016.

36 So z. B. § 1 LDSG SH.

37 So z. B. § 1 Nr. 2 HDSG v. 11.11.1986, Hess GVBl. I S. 309.

38 Simitis in Simitis (Fn. 6) Einleitung Rn. 21.

39 BVerfG U. v. 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 422.

40 Weichert in Däubler u. a. (Fn. 16) Art. 1 DSGVO Rn. 19 ff.

41 Initiative von Ende 2016, dokumentiert unter digitalcharta.eu.

42 Weichert in Däubler u. a. (Fn. 16) Art. 40 DSGVO Rn. 6 f.

43 G. v. 01.06.2017, BGBl. I S. 1416.

44 Krawczak/Weichert, Medizinforscher und Datenschützer fordern Bund-Länder-Staatsvertrag, DANA 2017, 193 ff. = Vorschlag einer modernen Dateninfrastruktur für die medizinische Forschung in Deutschland, www.netzwerk-datenschutzexpertise.de September 2017.

45 Weichert in Däubler u. a. (Fn. 16) § 29 BDSG Rn. 24 ff.

Anne Riechert

Das neue Recht auf Datenübertragbarkeit aus Sicht der Betroffenen

Mit dem neuen europäischen Recht auf Datenübertragbarkeit (Artikel 20 DSGVO) haben Sie das Recht, die von Ihnen bereitgestellten Daten von einem Anbieter direkt zu erhalten oder unmittelbar zu einem neuen Anbieter übermitteln zu lassen.

Die Frage ist allerdings, ob dadurch Ihr Recht auf informationelle Selbstbestimmung gestärkt wird.

Insgesamt besteht Uneinigkeit über Sinn und Zweck des Artikels 20 DSGVO. Die Regelung wird teilweise einschränkend dahin ausgelegt, dass (nur) die Datenübertragung von einem Dienstleister zum anderen erleichtert und Lock-In-Effekte vermieden werden sollen.[1] So bestand auch die ursprüngliche Intention der Europäischen Kommission darin, den Umzug eines Online-Profils von einem sozialen Netzwerk zu einem anderen zu erleichtern und diesem mit einem einzigen Klick zu ermöglichen.[2] Da diese Einschränkung aber im Wortlaut der Regelung des Artikel 20 DSGVO nicht erhalten ist, sollen damit grundsätzlich auch branchenübergreifende Datenübertragungen erfasst sein. Dies kann sich etwa auch auf eine Datenübermittlung von Ihrem Fitness-Tracker zu Ihrer Krankenversicherung beziehen.

Die Stiftung Datenschutz hat diese Fragen in ihrer Studie „Praktische Umsetzung des Rechts auf Datenübertragbarkeit" bereits umfassend untersucht.[3] In den folgenden Ausführungen werden die einzelnen Voraussetzungen des Rechts auf Datenübertragbarkeit nun aus Sicht des Betroffenen näher dargestellt. Es werden dabei vor allem die Leitlinien der Artikel-29-Datenschutzgruppe zum Recht auf Datenübertragbarkeit zugrunde gelegt, da sich die Datenschutzaufsichtsbehörden bei der Auslegung und Anwendung der Datenschutzgrundverordnung an diesen Empfehlungen orientieren werden.[4]

I. Um welche Daten geht es?

Gemäß Artikel 20 DSGVO ist es erforderlich, dass die personenbezogenen Daten entweder auf Grund einer informierten Einwilligung des Betroffenen oder auf der Grundlage eines Vertrags verarbeitet werden und vom Betroffenen *bereitgestellt* wurden.

Wesentlich und umstritten ist dabei das Merkmal des Bereitstellens, da es in der Datenschutzgrundverordnung nicht definiert ist.

Die Artikel-29-Datenschutzgruppe hat in ihrer Stellungnahme eine weite Auslegung vorgenommen. So sollen einerseits Buchtitel, die eine Person in einer Online-Buchhandlung gekauft hat, oder über einen Musik-Streaming-Dienst angehörte Musikstücke in den Anwendungsbereich des Rechts auf Datenübertragbarkeit fallen, da sie auf der Grundlage eines Vertrags verarbeitet werden.[5] Entsprechendes gilt für Daten, die die betroffene Person aktiv angibt, etwa durch Eintrag in ein Webformular. Andererseits sollen von den „bereitgestellten Daten" ebenso die so genannten „observed data" umfasst, also die Daten, die aufgrund der Inanspruchnahme eines Dienstes erzeugt werden, z.B. Nutzungsdaten, die Suchhistorie des Betroffenen oder Daten, die durch einen Fitness-Tracker aufgenommen worden sind.[6] Letzteres ist insbesondere von Unternehmen heftig kritisiert worden. Einigkeit besteht hingegen darüber, dass keine Daten erfasst sein sollen, die der Verantwortliche erst auf Grund der bereitgestellten Daten selbst ausgewertet und erzeugt hat („inferred data"), z.B. im Rahmen der Profilbildung und Scorewerte.[7]

II. Bereitgestellte Daten - Einzelfragen und Beispiele

In den folgenden Beispielen sind ebenfalls Überlegungen dahingehend zu finden, inwieweit ein mögliches Recht auf Datenübertragung tatsächlich auch zur Stärkung des informationellen Selbstbestimmungsrechts beiträgt und grundsätzlich in der Praxis Anwendung finden könnte.

1. Auskunfteien

Positivdaten

Für die Informationen, die bei Wirtschaftsauskunfteien gespeichert sind, könnte die Regelung des Artikel 20 DSGVO bedeuten, dass davon die Daten betroffen sind, die aufgrund einer Einwilligung der betroffenen Person an diese übermittelt wurden:

Hat der Kunde seiner Bank sein Einverständnis dahingehend erteilt, dass Daten über die Beantragung, die Aufnahme (Kreditnehmer und Kreditbetrag, Laufzeit und Ratenbeginn) und die vereinbarungsgemäße Abwicklung (z. B. vorzeitige Rückzahlung, Laufzeitverlängerung) des in Anspruch genommenen Kredits an eine Wirtschaftsauskunftei übermittelt werden dürfen, besteht dieser gegenüber auch ein entsprechender Anspruch auf Übertragung dieser Daten in einem strukturierten, gängigen und maschinenlesbaren Format.

Hier muss man auch davon ausgehen, dass diese Daten von der betroffenen Person bereitgestellt wurden, da sie in die Übermittlung eingewilligt und damit die Daten „aktiv und wissentlich" auch einem Dritten zur Verfügung gestellt hat. Die Übermittlung wurde seitens des Betroffenen also veranlasst. Ansonsten wäre es in diesem Falle nicht nachvollziehbar, wenn Daten nur dann als „bereitgestellt" gelten, sofern der Betroffene sie selbst übermittelt hat.

Ein Vermieter könnte beispielsweise dem potenziellen Mieter vorschlagen, die gewünschte Wohnung im Gegenzug einer unmittelbaren Datenübermittlung seitens der Wirtschaftsauskunftei zu vergeben. Mit Einwilligung der betroffe-

nen Person können ansonsten nur Vertragspartner der Wirtschaftsauskunftei unmittelbar auf diese Daten zugreifen, was bei privaten Vermietern jedoch regelmäßig nicht der Fall sein wird. Die Übertragung der Daten „mit einem Klick“ und in einem maschinenlesbaren Format an den Vermieter könnte den Rechtsverkehr vereinfachen, ohne den „Umweg“ über die Selbstauskunft und selbstständiger Bereitstellung eines entsprechenden Dokuments (in Papierform) an den Vermieter zu gehen.

Zum einen ist jedoch zu berücksichtigen, welchen Mehrwert diese Vorgehensweise für das informationelle Selbstbestimmungsrecht der betroffenen Person mit sich bringt und ob dieses damit tatsächlich gestärkt werden würde. Zum anderen ist sehr fraglich, ob der Vertragspartner ein Interesse daran hätte, da Positivdaten nur eine „halbe“ Information darstellen. Der Vertragspartner hat eher ein besonderes Interesse an den so genannten Negativdaten, also an Daten, die über nicht vertragsgemäßes Verhalten (fällige Forderungen, etc.) informieren. Nur wenn auch diese Daten von der Datenportabilität erfasst wären, würde ein entsprechender Anspruch überhaupt Sinn machen. Diese Frage wird unter dem folgenden Punkt „**Observed data?**“ behandelt.[8]

„Observed data“?

Eingangs wurde darauf hingewiesen, dass Daten, die aufgrund der Inanspruchnahme des Dienstes erzeugt werden, von den Datenschutzaufsichtsbehörden ebenfalls als „bereitgestellt“ eingeordnet werden. Solche Daten werden aufgrund von Aufzeichnungen der Aktivitäten der betroffenen Personen generiert.[9] Aber wie verhält es sich mit Informationen, die von Banken, Händlern, etc. an eine Wirtschaftsauskunftei aufgrund eines berechtigten Interesses übermittelt werden, beispielsweise Daten, die nicht vertragsgemäßes Verhalten betreffen (Konten- oder Kreditkartenmissbrauch oder sonstiges betrügerisches Verhalten) oder Daten über bestehende fällige Forderungen?

Hier stellt sich einerseits die Frage, welche personenbezogene Daten von Finanzeinrichtungen im Rahmen ihrer Pflicht zur Verhütung und Aufdeckung von Geldwäsche und anderen Formen der Finanzkriminalität verarbeitet werden, so dass von vorneherein kein Anspruch auf Datenportabilität besteht.[10]

Andererseits muss entschieden werden, ob diese Daten, wie etwa Informationen über bestehende fällige Forderungen, vom Betroffenen im Sinne von Artikel 20 DSGVO *„bereitgestellt“* wurden. Dies müsste gewissermaßen in analoger Betrachtung der oben beschriebenen Dienstnutzung bzw. Inanspruchnahme des Dienstes geschehen. Es müsste unterstellt werden können, dass bei dieser Fallkonstellation gleichermaßen Daten durch das Verhalten der betroffenen Person erzeugt werden. So werden die Informationen über betrügerisches Verhalten oder die fehlende Zahlungsfähigkeit oder Zahlungswilligkeit einer betroffenen Person aufgrund ihres Verhaltens während der Laufzeit des Vertrages durch das Kreditinstitut festgestellt. Dies kann darüber hinaus sogar erforderlich sein, da die Kreditwürdigkeit beurteilt werden muss, z.B. auch wenn durch das nicht vertragsgemäße Verhalten Umstände eintreten, die zur Kündigung des Vertrages berechtigen. Ob eine solche Verarbeitung mit einer Suchhistorie oder aufgezeichneten Pulswerten als vergleichbar eingestuft werden kann ist fraglich. Diesbezüglich sind den Ausführungen der Artikel-29-Datenschutzgruppe auch keine Hinweise zu entnehmen. Außerdem müsste die Verarbeitung mit „automatischen Mitteln“ erfolgen.[11] Selbst wenn man einen Datenübertragungsanspruch gemäß Artikel 20 DSGVO bejahen würde, stellt sich im Hinblick auf eine unmittelbare Übertragung der Daten an Dritte (etwa Vermieter) die Frage, ob eine solche brauchbare „Auskünfte“ liefert, da bei einem einzigen Verantwortlichen – anders als bei einer Wirtschaftsauskunftei – keine umfassenden Informationen über den Schuldner vorhanden sind.

Möchte sich die betroffene Person selbst über den Umfang der Verarbeitung ihrer personenbezogenen Daten durch einen Verantwortlichen (etwa einer Bank) erkundigen, könnte sie außerdem einen Auskunftsanspruch gemäß Artikel 15 DSGVO geltend machen, soweit sich aus § 34 BDSG (neu) nichts anderes ergibt.

Insgesamt ist hiervon zudem abzugrenzen, ob ein Anspruch gegen die Wirtschaftsauskunftei auf Datenübertragbarkeit bestehen kann. So erfolgte die Übermittlung solcher Negativdaten an eine Wirtschaftsauskunftei oder von dieser an weitere Dritte in der Vergangenheit stets aufgrund eines berechtigten Interesses. In diesem Falle kann keine Bereitstellung durch den Betroffenen unterstellt werden. Der Betroffene muss zwar in diesem Falle über die Datenübermittlung informiert werden. Eine Information, auch wenn sie ausführlich ist, ist jedoch etwas anderes als eine vorherige ausdrückliche Einwilligung. Daher ist bei einer Übermittlung aufgrund eines berechtigten Interesses regelmäßig davon auszugehen, dass die Weitergabe der Daten an den Dritten nicht auf Veranlassung des Betroffenen erfolgt ist.

Gegenüber der Wirtschaftsauskunftei kann seitens der betroffenen Person natürlich ebenfalls ein Auskunftsanspruch geltend gemacht werden (Artikel 15 DS-GVO). Daher wird es im Hinblick auf die Wirtschaftsauskunfteien wohl bei dem gängigen Verfahren verbleiben, dort eine Selbstauskunft einzuholen und diese bei Bedarf entsprechend weiterzuleiten.

Scorewert

Beim Scorewert handelt es sich um die Errechnung eines Wahrscheinlichkeitswertes auf der Grundlage des vorhandenen Datenbestandes, um das Kreditrisiko zu beurteilen. Dies fällt demgemäß unter den Begriff der „inferred data“, Daten, die der Verantwortliche erst auf Grund der bereitgestellten Informationen selbst ausgewertet und erzeugt hat.

Diese sind aber vom Auskunftsrecht umfasst, wenn auch die deutsche Rechtsprechung die Wahrung der Betriebs- und Geschäftsgeheimnisse im Rahmen der angewendeten Berechnungsmethode hervorhebt.[12] Eine andere Frage ist, ob ein solcher Scorewert überhaupt gebildet werden darf. Bei Auskunfteien richtet sich die Zulässigkeit nach § 31 BDSG (neu) und Artikel 6 Absatz 1f DS-GVO. Hier wird die Frage diskutiert, inwieweit § 31 BDSG (neu) europarechtswidrig und damit unanwendbar ist.[13] In diesem Falle bliebe es bei der Scorewert-Berechnung und der Weitergabe an Dritte allein bei Artikel 6 Absatz 1f DSGVO („berechtigte Interessen“).

Ergänzender Hinweis:

Im Rahmen eines Kaufvertrages stellt sich zudem die Frage, ob die Zugrundlegung eines (vorhandenen) Scorewerts seitens des Händlers für die Vertragserfüllung erforderlich ist. Zu bedenken ist jedoch, dass der Händler den Abschluss des Kaufvertrages in derselben Weise von einer anderen Zahlungsmöglichkeit abhängig machen könnte, etwa Kreditkarte oder Vorkasse. So würde dem Kunden der Rückgriff auf einen Scorewert „erspart", es sei denn dieser hätte eine informierte und freiwillige Einwilligung erteilt.[14] Der vorhandene Scorewert ist davon aber stets unabhängig zu betrachten: Dieser wurde „nur" aufgrund eines berechtigten Interesses sowie auf der Grundlage von bereitgestellten Daten seitens des jeweils Verantwortlichen eigenständig gebildet. Der Scorewert ist damit nicht Gegenstand des Rechts auf Datenübertragbarkeit, wohl aber des Auskunftsanspruches (Artikel 15 DS-GVO), wenn auch wie gerade ausgeführt unter Beachtung des Geschäftsgeheimnisses einer Wirtschaftsauskunftei.

2. Telekommunikationsdaten

Bei der Nutzung eines Telekommunikationsdienstes fallen so genannte Verkehrsdaten/Verbindungsdaten (z.B. Nummer und Kennung der Anschlüsse oder Standortdaten) an. Im Entwurf der E-Privacy-Verordnung findet sich nun dazu der Begriff der Kommunikationsmetadaten.[15] Dies sind Daten, die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden. Im Einzelnen zählen dazu die zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts einer Kommunikation verwendeten Daten und die erzeugten Daten über den Standort des Geräts sowie Datum, Uhrzeit, Dauer und Art der Kommunikation.[16]

In Bezug auf das Recht auf Datenübertragbarkeit sind Telekommunikationsunternehmen der Auffassung, dass Verkehrsdaten aufgrund der jeweiligen Dienstnutzung zwangsläufig entstehen und daher nicht von den betroffenen Personen bereitgestellt werden. Der Verband BitKom verweist in diesem Zusammenhang darauf, dass Verkehrsdaten nicht vom Recht auf Datenübertragbarkeit erfasst sein dürfen, u.a. aus dem Grunde, da zum einen Schutzrechte von Dritten betroffen seien und zum anderen die Verkehrsdaten bei einem Kommunikationsvorgang stets und ohne Zutun der Betroffenen anfallen und damit nicht für die Vertragserfüllung erforderlich seien.[17]

Die Artikel-29-Datenschutzgruppe sieht dies jedoch anders und stuft Verkehrs- und Standortdaten als vom Nutzer bereitgestellte Daten im Sinne von Nutzungsdaten ein.[18] Damit stünde der betroffenen Person auch ein grundsätzliches Recht auf Übertragung dieser Daten zu.

Insgesamt ist außerdem der Entwurf der E-Privacy-Verordnung zu beachten. Im Sinne dieser Regelung ist es möglich, dass die Verarbeitung dieser „Verkehrsdaten" (im Sinne der oben beschriebenen Kommunikationsmetadaten) aufgrund einer Einwilligung der Betroffenen erfolgen muss.[19] Erfolgt also eine Verarbeitung solcher Kommunikationsmetadaten (Verkehrs- und Standortdaten) aufgrund einer Einwilligung der betroffenen Person, wäre gemäß des Wortlauts des Artikels 20 DSGVO auch aus diesem Grunde ein Anspruch auf Übertragung dieser Daten zu einem anderen Dienstleister gegeben.[20]

Ansonsten stellt sich allerdings die Frage der praktischen Relevanz für das Recht auf Datenübertragbarkeit aufgrund der durch die E-Privacy-Verordnung vorgegebenen engen Grenzen einer zulässigen Speicherung von Kommunikationsdaten. Dies könnte allenfalls mit Blick auf die Vorratsdatenspeicherung relevant sein,[21] wobei zu berücksichtigen ist, dass in der Vergangenheit die Bundesnetzagentur sogar ein Auskunftsrecht gemäß § 34 BDSG aufgrund der möglichen Beeinträchtigung Dritter abgelehnt hat.[22] So werden Verkehrsdaten in Bezug auf einen bestimmten Anschluss gespeichert und berühren damit die Interessen des Anschlussinhabers sowie die Interessen von Mitbenutzern oder des Kommunikationspartners. Diese Wertung sollte ebenso bei der Datenportabilität gemäß Artikel 20 Datenschutzgrundverordnung beachtet werden.[23]

3. Cookies

Die Datenschutzkonferenz hat in ihrem Papier zur Positionsbestimmung ausgeführt,[24] dass es einer vorherigen Einwilligung bei der Erstellung von Nutzerprofilen sowie beim Einsatz von Tracking-Mechanismen bedürfe, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen. Das bedeutet, dass eine informierte Einwilligung i. S. d. DSGVO, in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung vor der Datenverarbeitung eingeholt werden muss, d. h. z.B. bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.

Nach dem Wortlaut des Artikel 20 DS-GVO würde dementsprechend das Setzen eines Cookies unter Einwilligung auch einen entsprechenden Anspruch auf Datenübertragbarkeit gegenüber dem Dritten auslösen, der dieses Cookie für seine Zwecke verwendet. Grundsätzlich stellt sich allerdings die Frage, „wie" der Dritte diese Daten verarbeitet. Regelmäßig wird er eine „zumindest pseudonymisierte" Profilbildung vornehmen. Dies heißt, er würde einen Datenbestand schaffen, der gemäß der Auffassung der Aufsichtsbehörden als „inferred data" zu bewerten ist. Nur wenn Rohdaten beim Dritten vorhanden sind, die dieser noch nicht gelöscht hat, bestünde ein Anspruch auf Datenübertragbarkeit auch gegenüber dem Dritten. Allerdings ist bei pseudonymisierter Erhebung Artikel 11 DSGVO zu berücksichtigen, so dass geprüft werden muss, ob für den Verantwortlichen eine Identifikation möglich ist. In diesem Falle besteht ein Recht auf Datenübertragbarkeit nur dann, wenn der Nutzer zusätzliche Informationen bereitstellt, die seine Identifizierung erlauben.

In Bezug auf die Verwendung von eigenen Tracking-Maßnahmen bzw. Webanalysediensten durch einen Verantwortlichen sieht der Entwurf der E-Privacy-Verordnung deren Zulässigkeit ohne weitere Einschränkung vor. Dies umfasst nicht nur Cookies, sondern auch Fingerprints, sofern diese Technologien zur Besuchermessung eingesetzt werden. Der Nutzer muss hierin also nicht einwilligen, so dass das Recht

auf Datenübertragbarkeit nur berührt ist, sofern man diese Daten als „observed data" einordnet. Werden diese jedoch pseudonymisiert erhoben, gelten die gerade gemachten Überlegungen. Generierte Profilbildungen des Verantwortlichen sind nicht von der Datenportabilität umfasst. Ansonsten müssten vorhandene Rohdaten einem Nutzer in dem Sinne zugewiesen sein, dass er auch identifizierbar ist (Artikel 11 DS-GVO).[25]

Ergänzender Hinweis

Nicht abschließend geklärt ist, was unter „einer sonstigen eindeutigen bestätigenden Handlung" im Rahmen der Einwilligung gemäß Artikel 4 Nr. 11 DSGVO zu verstehen ist. Sofern in diesem Sinne auch eine (transparente) Information der Nutzer auf der Webseite des Verantwortlichen dahingehend ausreichen sollte, dass Cookies verwendet werden, könnte seine eindeutig bestätigende Handlung in der Weiternutzung des Dienstes liegen. Dies hieße, dass der Nutzer nicht aktiv einen Haken dahingehend setzen muss, dass er mit den Cookies einverstanden ist, sondern er müsste die Informationen über die Cookies lesen und weitersurfen.[26] Die Artikel-29-Datenschutzgruppe hat in ihrer Orientierungshilfe zu den Voraussetzungen einer Einwilligung zwar ausgeführt, dass die „bloße Weiternutzung eines Dienstes keine eindeutig bestätigende Handlung sei".[27] Die aktuelle Praxis in den Mitgliedstaaten in Bezug auf die Zulässigkeit von Cookies wird jedoch unterschiedlich gehandhabt und zeigt, dass hierauf besonderes Augenmerk gelegt werden sollte.[28] So veröffentlicht selbst die britische Datenschutzbehörde ICO auf ihrer Webseite lediglich folgenden Hinweis (den der Nutzer auch ignorieren kann)[29]:

"*We have placed cookies on your device to help make this website better. You can use this tool to change your cookie settings. Otherwise, we'll assume you're OK to continue*."

Erst bei einem weiteren Klick auf "Information and settings" erhält man als Nutzer auch eine Information über verwendete „Third Party Cookies", welche seitens des Nutzers aktiv ausgeschaltet werden müssen.

„*To control third party cookies, you can also adjust your browser settings*[30]".

Nicht geklärt ist, was unter „einer sonstigen eindeutigen bestätigenden Handlung" im Rahmen der Einwilligung gemäß Artikel 4 Nr. 11 DSGVO zu verstehen ist. Sofern in diesem Sinne auch eine Information der Nutzer auf der Webseite des Verantwortlichen ausreichen sollte, dass Cookies verwendet werden, würde seine eindeutig bestätigende Handlung in der Weiternutzung des Dienstes bestehen. Dies hieße, dass der Nutzer nicht aktiv einen Haken dahingehend setzen muss, dass er mit den Cookies einverstanden ist, sondern er müsste die Informationen über die Cookies lesen und weitersurfen.[31]

Die aktuelle Praxis in den Mitgliedstaaten in Bezug auf die Zulässigkeit von Cookies wird unterschiedlich gehandhabt.[32] In der Vergangenheit wurde zudem auch bereits die Auffassung vertreten, dass der Wortlaut des § 15 Telemediengesetzes im Widerspruch zu den europäischen Vorgaben stehe.[33] Dies wurde nun durch das Papier der Datenschutzkonferenz nochmals bestätigt.

Die Europäische Kommission hat im Übrigen die Vorstellung, dass die „Cookie-Thematik" zukünftig durch Browserlösungen geregelt werden soll, die entsprechende Einstellungsmöglichkeiten bieten.[34] Allerdings müssen solche technischen Lösungen erst noch entwickelt werden…

4. Soziale Netzwerke

Der eigentlichen bzw. ursprünglichen Intention der Europäischen Kommission, dass das Recht auf Datenübertragbarkeit den Wechsel von sozialen Netzwerken zu datenschutzfreundlichen Technologien verwirklichen soll, stehen in der Praxis regelmäßig die Rechte Dritter entgegen. Ein solches Ansinnen ist nur umsetzbar, wenn zumindest alle „Freunde" der betroffenen Person ebenso das Netzwerk wechseln. Hinderungsgrund ist hier stets das Merkmal des Bereitstellens. Daten aus Chatprotokollen oder Profilbilder von Dritten sind nicht von der betroffenen Person bereitgestellt und bedürfen einer entsprechenden Einwilligung, wenn sie übermittelt werden sollen.[35] Die Artikel-29-Datenschutzgruppe bezieht sich in ihrer Stellungnahme auf Kontaktlisten, so dass beispielsweise ein Webmail-Dienst die Erstellung eines Verzeichnisses mit den Kontakten, Freunden, Verwandten, Familienangehörigen und dem weiteren Umfeld der betroffenen Person ermöglichen könne.[36] Dies führe dazu, dass Verantwortliche das gesamte Verzeichnis der ein- und ausgehenden E-Mails an die betroffene Person übertragen könnten.[37]

Wenn diese Daten jedoch bei einem kommerziellen Anbieter gespeichert werden, den sich die betroffenen Dritten nicht bewusst und eigenständig ausgesucht haben, ist diese Ansicht zu hinterfragen. Dies gilt nun für die betroffenen Dritten einer Datenportabilität. Es könnte zum jetzigen Zeitpunkt verfrüht sein, dem neuen Verantwortlichen die verantwortungsbewusste Löschung und Nichtnutzung von Daten Dritter zu übertragen, wie von der Artikel-29-Datenschutzgruppe gefordert. Diese Auffassung, dass auch Daten Dritter grundsätzlich übermittelt, aber nicht für eigene Zwecke der neuen Datenverantwortlichen genutzt werden dürfen, zieht nicht in Betracht, dass bereits in der Übertragung der Daten ein Verstoß gegen das informationelle Selbstbestimmungsrecht liegen kann.[38] Möglich wäre etwa, dass sich der Dritte bewusst gegen einen kommerziellen Anbieter entschieden hat. Der Vorschlag der Einführung von Tools, mit denen die betroffenen Personen Daten auswählen und ausschließen können[39], ist an dieser Stelle nur ausreichend, wenn die Drittbetroffenen damit zuvor ihr Einverständnis erklären können, dass ihre Daten zu einem weiteren kommerziellen Anbieter übertragen werden.[40] Dann müsste jedoch eine entsprechende Verpflichtung im Hinblick auf die Einführung solcher Tools etabliert werden und die Transparenz sichergestellt sein.

Etwas anderes könnte insgesamt gelten, wenn der Nutzer beispielsweise seine Kontaktliste oder seinen Facebook-Account auf sein eigenes, privates Gerät kopieren möchte,[41] da es sich in diesem Falle tatsächlich um eine „ausschließlich" private Verarbeitung handelt.

III. Um welche Dienste geht es?

Die Artikel-29-Datenschutzgruppe hat in ihren Ausführungen keine Einschränkungen gemacht: Der Anspruch

auf Datenübertragbarkeit gilt sowohl für alle vertragsrelevanten Daten als auch für alle Daten, die aufgrund des Verhaltens der betroffenen Person erzeugt wurden sowie für Daten, die mittels Einwilligung bereitgestellt wurden. Damit ist grundsätzlich auch eine branchenübergreifende Datenübertragung umfasst, soweit sich zukünftig keine andere Rechtspraxis, etwa durch ausgearbeitete Verhaltensregeln oder anderslautende Empfehlungen des Europäischen Datenschutzes herausbildet.

Es sind daher Geschäftsmodelle denkbar, die eine Rabattierung der monatlichen Gebühr gegen den Erhalt von Daten vorsehen. Damit ist auch ein Datenhandel verbunden, wobei die betroffenen Personen natürlich immer gut überlegen sollten, wem sie für welchen Preis ihre Daten anvertrauen. Dies gilt umso mehr, da der Wert der Daten zum aktuellen Zeitpunkt noch gar nicht bezifferbar ist. Hier spielt außerdem eine Rolle, inwieweit Artikel 20 DSGVO einen wirtschaftlichen Vorteil des informationellen Selbstbestimmungsrechts umfassen und diesen schützen soll.[42] In diesem Zusammenhang stellt sich die zusätzliche Frage nach der Kommerzialisierung von Daten und ob den betroffenen Personen eine wirtschaftliche Verwertungsbefugnis zusteht,[43] aber gleichwohl, ob sie diese überhaupt selbstbestimmt ausüben können, wenn sie den Wert der Daten nicht kennen.

IV. Wie sind die Daten an die betroffene Person zu übermitteln?

Die Daten sind in einem interoperablen und strukturierten, gängigen, maschinenlesbaren Format an die betroffene Person zu übermitteln. Die Aufforderung der Artikel-29-Datenschutzgruppe, interoperable Formate zu entwickeln,[44] stellt zwar ebenso wenig eine rechtliche Verpflichtung dar wie die entsprechende Regelung in Erwägungsgrund 68 der Datenschutzgrundverordnung.[45] Allerdings müssen die Verantwortlichen den betroffenen Person die Ausübung ihrer Rechte erleichtern (Artikel 12 Absatz 2 Satz 1 DSGVO) und Aufsichtsbehörden können Verantwortliche anweisen, den Anträgen der betroffenen Personen zu entsprechen (Artikel 58 Absatz 2c DSGVO). Es wird zudem darauf verwiesen, dass die Nachfrage der Nutzer nach Interoperabilität einen wirtschaftlichen Druck auf die Dienstleister erzeugen könne.[46] Allerdings ist zu berücksichtigen, dass geeignete Formate bereits existieren und in der Datenübertragbarkeit keine technische Hürde gesehen wird.[47] Die Verantwortlichen können die personenbezogenen Daten in offenen Formaten (wie XML, JSON oder CSV) bereitstellen, sofern es für eine gegebene Branche oder für einen gegebenen Kontext keine gängigen Formate geben sollte.[48]

Ein Dokument gilt als maschinenlesbar, wenn es in einem Dateiformat vorliegt, das so strukturiert ist, dass Softwareanwendungen die konkreten Daten, einschließlich einzelner Sachverhaltsdarstellungen und deren interner Struktur, einfach identifizieren, erkennen und extrahieren können.[49] Bei einem maschinenlesbaren Format geht es daher vorrangig um die automatisierte Auslesbarkeit und Verarbeitbarkeit durch Software.[50] So lehnt Artikel-29-Datenschutzgruppe pdf-Fassungen eines E-Mail-Eingangsfachs als ausreichend strukturiertes Format ab, da es nicht die Wiederverwendung der Daten ermöglicht.[51]

V. Abgrenzung zum Auskunftsrecht

Das Auskunftsrecht (Artikel 15 DSGVO) ist zwar grundsätzlich nicht mit dem Recht auf Datenübertragbarkeit zu verwechseln. Dennoch ist der Historie des Gesetzgebungsverfahrens zu entnehmen, dass das Recht auf Datenübertragbarkeit ursprünglich als Verbesserung des Auskunftsrechts gedacht war.[52] Im ersten Entwurf einer Datenschutzgrundverordnung (2012) umfasste das Recht auf Datenübertragbarkeit einen Anspruch auf Kopie sämtlicher (verarbeiteter) Daten in einem gängigen elektronischen Format, was nun in der geltenden Fassung in Artikel 15 Absatz 3 DSGVO (Auskunftsanspruch) geregelt ist.[53]

Der Unterschied zwischen dem Recht auf Datenübertragbarkeit und dem Auskunftsanspruch besteht auch in den jeweiligen Formaten. In Artikel 15 Absatz 3 DSGVO ist geregelt, dass bei elektronischer Antragstellung die Auskunft in einem gängigen elektronischen Format zu erteilen ist, während beim Recht auf Datenübertragbarkeit ein maschinenlesbares Format gefordert ist. Eine Auskunft kann daher auch in einem pdf-Dokument im Sinne eines gängigen elektronischen Formats erfolgen, während dies beim Recht auf Datenübertragbarkeit regelmäßig nicht möglich ist (siehe hierzu insbesondere auch die obigen Ausführungen unter IV.).

Eine andere Frage ist es, inwiefern das informationelle Selbstbestimmungsrecht aufgrund eines Rechts auf Datenübertragbarkeit gestärkt wird. Ob dem Betroffenen zusätzlich zu seinem Auskunftsrecht auch ein Recht auf Datenübertragbarkeit zusteht, hängt von der Rechtsgrundlage der Verarbeitung ab. Nur bei vertragsrelevanten Daten und bei Daten, die mit Einwilligung verarbeitet werden, kommt ein solches Recht überhaupt in Betracht. Daher kann die Frage auch gegenteilig dahingehend gestellt werden, ob das informationelle Selbstbestimmungsrecht des Betroffenen eingeschränkt ist, wenn ihm nur ein Auskunftsanspruch zusteht, etwa wenn Daten nicht aufgrund einer Einwilligung, sondern aufgrund berechtigter Interessen verarbeitet werden. Zu bedenken sind hier jedoch die folgenden Überlegungen: Es vereinfacht zwar insoweit den Rechtsverkehr, wenn Daten direkt an Dritte übermittelt werden. Das Grundrecht auf Datenschutz wäre jedoch bereits genüge getan, wenn die betroffene Person darüber im Bilde ist, wer welche Daten zu welchem Zweck über sie verarbeitet und sie in die Lage versetzt wird, diese Informationen selbstbestimmt an Dritte weiterzugeben (etwa eine Bonitätsauskunft an den Vermieter). Dies könnte aber auch durch einen Ausdruck der Daten in einem Papierformat oder im Rahmen eines übermittelten pdf-Dokuments erfolgen. Die Maschinenlesbarkeit des Formats und die Datenübertragung „mittels eines Klicks" stellen ein fortschrittliches Mittel für die betroffenen Personen dar, ihr Recht einfacher auszuüben, aber sind im eigentlichen Sinne für die Verwirklichung ihres informationellen Selbstbestimmungsrechts nicht unbedingt notwendig.

Eine Stärkung des informationellen Selbstbestimmungsrechts ist aber in den Fällen zu bejahen, in denen ein An-

bieterwechsel und/oder ein Umzug des kompletten Datenbestandes, insbesondere ein Wechsel zu datenschutzfreundlichen Technologien erfolgen soll. Ein solches Vorhaben darf nicht daran scheitern, dass die personenbezogenen Daten nicht so verwendet werden können, wie es der Betroffene vorsieht.

VI. Unentgeltlichkeit

Die Verpflichtung des Verantwortlichen, dem Recht auf Datenübertragbarkeit unentgeltlich nachzukommen, ergibt sich aus Artikel 12 Absatz 5 DSGVO. Nur bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder ein angemessenes Entgelt verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. Für das Merkmal „exzessiv" müssen noch praxistaugliche Auslegungskriterien entwickelt werden. Im Übrigen bietet die SCHUFA auf ihrer Seite gegen monatliche Gebühr die Möglichkeit an, die gespeicherten Daten jederzeit online einzusehen. Dies betrifft zwar das Auskunftsrecht. Aber mit Blick auf künftige Geschäftsmodelle könnte die Frage gestellt werden, ob beispielsweise bei monatlicher Übertragung der Daten einer FitnessApp an eine Krankenversicherung eine entsprechende Gebühr wegen „exzessiver Anträge" in Betracht kommen darf.

VII. Geltendmachung des Rechts

Die betroffene Person kann beim Verantwortlichen einen Antrag stellen. Hier besteht Formfreiheit. Dennoch empfiehlt es sich für die Betroffenen schon aufgrund der in Artikel 12 Absatz 3 und Absatz 4 DSGVO geregelten Fristen, den Antrag schriftlich oder zumindest per E-Mail zu stellen. Sofern die betroffene Person ihre Identität nicht nachweisen kann, kann der Verantwortliche die Datenübertragung zudem verweigern (Artikel 12 Absatz 2 DSGVO).

Sofern der Verantwortliche die Datenübertragung ablehnt, muss er dies begründen. Gemäß Artikel 12 Absatz 4 DSGVO unterrichtet er die betroffene Person insoweit ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen. Ein Grund der Verweigerung könnte etwa die technische Machbarkeit darstellen. Hierbei handelt es sich um einen unbestimmten Rechtsbegriff, der subjektiv als auch objektiv ausgelegt werden kann.[54] Eine objektive Auslegung könnte kleine und mittelständische Unternehmen belasten, sofern die individuelle Leistungsfähigkeit keine Rolle spielt. Daher wird derzeit darauf verwiesen, dass sich die technische Machbarkeit nach den beim Verantwortlichen schon vorhandenen technischen Möglichkeiten sowie nach der wirtschaftlichen Verhältnismäßigkeit richten soll. [55] Hierzu gibt es insgesamt zwar noch keine konsolidierte Auffassung. Es wird jedoch eine Mitwirkung des Verantwortlichen in verhältnismäßigen Umfang verlangt, etwa bei der Anpassung der Übertragungsformate.[56]

Die Aufsichtsbehörde hat im Übrigen die Möglichkeit, den Verantwortlichen anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen (Artikel 58 Absatz 2c DSGVO). Davon ist dementsprechend auch das Recht auf Datenübertragbarkeit umfasst. Möchte die betroffene Person das Recht auf Datenübertragbarkeit gerichtlich durchsetzen, können je nach Anspruchsgegner unterschiedliche Gerichte zuständig sein (Zivilgericht, Arbeitsgericht, Sozialgericht, Verwaltungsgericht, Finanzgericht).[57]

In jedem Falle muss der Betroffene berücksichtigen, dass mit der Geltendmachung seines Rechts auf Datenübertragbarkeit keine Löschung seiner Daten verbunden ist. Dieses Recht muss er zusätzlich ausüben. Dies ist vor allem zu beachten, wenn die unmittelbare Übertragung von einem Verantwortlichen auf den anderen aufgrund eines Wechsels des Dienstes verlangt wird, mit der nicht die automatische Löschung des Datenbestandes bei dem ursprünglichen Dienstleister verbunden ist.

Fazit

Das Recht auf informationelle Selbstbestimmung kann insgesamt dadurch besonders gestärkt werden, wenn mit der Geltendmachung des Rechts auf Datenübertragbarkeit zugleich die Möglichkeit des Selbstdatenschutzes oder ein Wechsel des Datenbestandes zu datenschutzfreundlichen Technologien verbunden wird.[58] Es wird der Rahmen für viele neue Dienste geschaffen, die den Verbrauchern zugutekommen können. So sind Rabattmodelle als Gegenleistung für die Übertragung von personenbezogenen Daten denkbar. Hier muss die betroffene Person allerdings besonderes Augenmerk darauf legen, wem sie ihre Daten zu welchem Preis anvertraut und vor allem stets daran denken, dass mit der Datenportabilität keine automatische Löschung der Daten beim ursprünglichen Dienstleister erfolgt.

In Abgrenzung zum Auskunftsrecht muss beim Recht auf Datenübertragbarkeit im Übrigen genau differenziert werden, auf welcher Rechtsgrundlage die Datenverarbeitung erfolgt ist: Nur bei Einwilligung, bei Daten, die zur Vertragserfüllung erforderlich sind oder bei Daten, die die betroffene Person aufgrund ihres Verhaltens bzw. ihrer Aktivitäten generiert hat, besteht ein Anspruch auf Datenübertragbarkeit. Daher ist bei einer Datenverarbeitung aufgrund eines berechtigten Interesses von vorneherein ein Anspruch auf Datenübertragbarkeit auszuschließen.

In einigen bisherigen Geschäftsfeldern wird das Recht auf Datenübertragbarkeit darüber hinaus bereits aus rein praktischen Erwägungen keine Rolle spielen. Im Übrigen ist im Einzelfall denkbar, dass das informationelle Selbstbestimmungsrecht der betroffenen Person durch das Auskunftsrecht ebenso gut umgesetzt wird.

1 Siehe hierzu Hennemann, Ping 01.17, S. 6 mit Verweis auf Erwägungsgrund 68 der Datenschutzgrundverordnung.

2 Siehe Jüllicher/Röttgen/v.Schönfeld, ZD 2016, S. 360. Bei der Datenübertragung auf eine andere automatisierte Anwendung wurde der Fokus auf soziale Netzwerke gelegt und die betroffene Person hatte einen Anspruch auf Übertragung der vertragsrelevanten Daten bzw. der Daten, die mit ihrer Einwilligung zur Verfügung gestellt wurden. Siehe Jüllicher/Röttgen/v.Schönfeld, ZD 2016, S.360/362; Hennemann, Ping 01.17., S. 6; Strubel, ZD 8/2017, S. 359 mit dem

Hinweis, dass ursprünglich angedacht war, das Recht auf Datenübertragbarkeit auf die Angebote Sozialer Medien zu begrenzen; Schätzle, Ping 02.16, S. 74 mit dem Hinweis auf die Kritik, dass es bei dem Recht auf Datenübertragbarkeit nicht um den Schutz der Privatsphäre gehe, sondern es sich vielmehr um ein wettbewerbspolitisches Instrument handele. Hennemann, Ping 01.17., S. 6 mit Verweis auf den wettbewerblichen Ansatz sowie auf die Aussage von Jan Albrecht (Berichterstatter des Europäischen Parlaments zur Datenschutzgrundverordnung), der in Artikel 20 einen Katalysator eines Wettbewerbs um datenschutzfreundliche Technologien sieht.

3 Siehe Stiftung Datenschutz, https://stiftungdatenschutz.org/themen/datenportabilitaet/.

4 Artikel-29-Datenschutzgruppe, WP 242 Guidelines on the right to data portability vom 13.12.2016 und Artikel-29-Datenschutzgruppe, WP 242 Guidelines on the right to data portability vom 05.04.2017

5 Artikel-29-Datenschutzgruppe, WP 242, S. 8.

6 Artikel-29-Datenschutzgruppe, WP 242, S. 11/12; Benedikt, RDV 2017, S. 190; Jüllicher/Röttgen/v.Schönfeld, ZD 2016, S. 359, die ein aktives Tun als Voraussetzung ablehnen.

7 Artikel-29-Datenschutzgruppe, WP 242, S.10.

8 Ergänzender Hinweis: Für die betroffenen Personen empfiehlt es sich insgesamt, die Entwicklung der (europaweiten) Praxis im Auge zu behalten. So wird in Bezug auch auf die Übermittlung von positiven Vertragsdaten an Wirtschaftsauskunfteien vertreten, dass keine Einwilligung erforderlich sei, sondern diese aufgrund eines berechtigten Interesses erfolgen darf (Buchner/Petri in: Kühling/Buchner, DS-GVO – BDSG, Artikel 6 DS-GVO Rn. 164.) Daher muss man bei einer Übermittlung aufgrund eines berechtigten Interesses regelmäßig davon ausgehen, dass die Weitergabe der Daten an den Dritten nicht auf Veranlassung des Betroffenen erfolgt ist (siehe auch die nachfolgenden Ausführungen unter „observed data").
Dem Betroffenen steht jedoch in jedem Falle ein Auskunftsanspruch zu (Artikel 15 DSGVO).

9 Herbst in: Kühling/Buchner, DS-GVO – BDSG, Artikel 20 DS-GVO Rn. 11.

10 Artikel-29-Datenschutzgruppe, WP 242, S. 10.

11 Artikel-29-Datenschutzgruppe, WP 242, S. 10. Herbst in: Kühling/Buchner, DS-GVO – BDSG, Artikel 20 DS-GVO Rn. 13 weist darauf hin, dass durch diese Einschränkung dem Verantwortlichen der Aufwand erspart wird, etwaige nicht maschinenlesbare Aufzeichnungen in maschinenlesbare Daten umzuwandeln.

12 BGH, Urteil vom 28. Januar 2014, Aktenzeichen: VI ZR 156/13. Der BGH vertritt die Auffassung, dass das gesetzgeberische Ziel eines transparenten Verfahrens dadurch erreicht wird, dass für den Betroffenen ersichtlich ist, welche konkreten Umstände als Berechnungsgrundlage in die Ermittlung des Wahrscheinlichkeitswerts eingeflossen sind. Aber etwa die Gewichtung der in den Scorewert eingeflossenen Merkmale muss jedoch im Rahmen eines Auskunftsersuchens nicht benannt werden. Im Übrigen versucht die Initiative „OpenSCHUFA" gerade per Crowdfunding Gelder für ein Projekt zu sammeln, in welchem eine Auswertungs-Software hinsichtlich des von der SCHUFA verwendeten Algorithmus entwickelt wird. Es sollen mögliche Fehler im Algorithmus sowie innerhalb der Schnittstellen zu den Vertragspartnern untersucht werden.

13 Buchner in: Kühling/Buchner, DS-GVO – BDSG, § 31 BDSG Rn. 6.

14 In diesem Sinne auch Buchner/Petri in: Kühling/Buchner, DS-GVO – BDSG, Artikel 6 DS-GVO Rn. 66.

15 Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.01.2017 (E-Privacy-Verordnung). Gemäß Artikel 95 der Datenschutzgrundverordnung werden natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auferlegt, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen. Die E-Privacy-Verordnung ist die Nachfolgeregelung und präzisiert und ergänzt durch die Festlegung besonderer Vorschriften die Datenschutzgrundverordnung.

16 Siehe Artikel 4 Absatz 3 c) des Entwurfs der E-Privacy-Verordnung.

17 Bitkom, Stellungnahme Datenportabilität, S. 10 mit dem Verweis unter anderem darauf, dass Verkehrs- und Standortdaten als Folge standardisierter Protokolle anfallen und nicht am Willen der Beteiligten hängen, sondern vom Kommunikationsvorgang initiiert werden. Abrufbar unter https://www.bitkom.org/noindex/Publikationen/2017/Positionspapiere/20170411-Stellungnahme-Datenportabilitaet-Fin.pdf

18 Artikel-29-Datenschutzgruppe, WP 242 S. 11.

19 Artikel 6 Absatz 2c) der E-Privacy-Verordnung.

20 Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern die Verarbeitung auf einer Einwilligung beruht.

21 Im Übrigen ergreift die Bundesnetzagentur zurzeit bzw. nach § 113b TKG keine Maßnahmen (Bußgeld), um die Verpflichtung zur Vorratsdatenspeicherung umzusetzen, siehe https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html;jsessionid=D4F71FC38673C1A16E69195D6334AA05

22 Das Auskunftsrecht besteht gemäß § 34 Abs. 4 i.V.m. § 33 Abs. 2 Satz 1 Nr. 3 BDSG nicht, wenn die Daten nach einer Rechtsvorschrift oder wegen des überwiegenden rechtlichen Interesses eines Dritten geheim gehalten werden müssen.

23 Fraglich ist allenfalls, ob es seitens der Telekommunikationsunternehmen praktikabel wäre, eine Bestätigung der betroffenen Person zu verlangen, dass keine Rechte Dritter betroffen sind: Der Anschlussinhaber ist für den Datenschutz der Mitbenutzer verantwortlich. Infolgedessen könnte ebenso eine entsprechende Bestätigung eingeholt werden, dass Mitbenutzer entweder ihre Einwilligung erteilt haben oder keine Mitbenutzer vorhanden sind.

24 https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf

25 Der Abänderungsvorschlag des Europäischen Parlaments sieht im Übrigen vor, dass nur aggregierte Daten verwendet und keine personenbezogenen Daten an Dritte übermittelt werden dürfen. Siehe den Vergleich der Fassungen der E-Privacy-Verordnung von EU-Kommission und EU-

Parlament unter https://www.lda.bayern.de/media/eprivacy_synopse.pdf

26 Siehe Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz“ und die rechtliche Stellungnahme zu der Thematik (Anne Riechert), S. 16 ff, insbesondere S. 20. (https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Stellungnahme_Rechtliche_Aspekte_eines_Einwilligungsassistenten_Anhang_1_final.pdf).

27 Artikel-29-Datenschutzgruppe, Guidelines on Consent under Regulation 2016/679 (wp259rev.01), S. 16, abrufbar unter http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030.

28 Siehe Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz“. Die enthaltene rechtliche Stellungnahme zu der Thematik (Anne Riechert), abrufbar unter https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Stellungnahme_Rechtliche_Aspekte_eines_Einwilligungsassistenten_Anhang_1_final.pdf enthält auf S. 16 ff. Ausführungen zur Umsetzung der Richtlinie 2002/58 EG (2009/136/EG) und der Praxis in Mitgliedstaaten in der EU.

29 https://ico.org.uk/

30 https://ico.org.uk/global/cookies/

31 Siehe Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz“ und die rechtliche Stellungnahme zu der Thematik (Anne Riechert), S. 16 ff, insbesondere S. 20. (https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_0032017/stiftungdatenschutz_Stellungnahme_Rechtliche_Aspekte_eines_Einwilligungsassistenten_Anhang_1_final.pdf).

32 Siehe Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz“. Die enthaltene rechtliche Stellungnahme zu der Thematik (Anne Riechert), abrufbar unter https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Stellungnahme_Rechtliche_Aspekte_eines_Einwilligungsassistenten_Anhang_1_final.pdf enthält auf S. 16 ff. Ausführungen zur Umsetzung der Richtlinie 2002/58 EG (2009/136/EG) und der Praxis in Mitgliedstaaten in der EU.

33 Siehe Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz“ und die rechtliche Stellungnahme zu der Thematik (Anne Riechert), S. 17 (https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Stellungnahme_Rechtliche_Aspekte_eines_Einwilligungsassistenten_Anhang_1_final.pdf).

34 Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.01.2017 (E-Privacy-Verordnung).

35 Herbst in: Kühling/Buchner, DS-GVO – BDSG, Artikel 20 DS-GVO Rn. 11.

36 Artikel-29-Datenschutzgruppe, WP 242 S. 13.

37 Artikel-29-Datenschutzgruppe, WP 242 S. 13.

38 Artikel-29-Datenschutzgruppe, WP 242, S. 14.

39 Artikel-29-Datenschutzgruppe, WP 242, S. 14.

40 In diesem Zusammenhang wird außerdem angemerkt, dass ein wirtschaftlich unverhältnismäßiger Aufwand entstünde, wenn die Betreiber Sozialer Netzwerke den Drittbezug manuell aussortieren müssten. Daher müssten entsprechende Algorithmen entwickelt werden. Siehe hierzu die Ausführungen von Jüllicher/Röttgen/v.Schönfeld, ZD 2016, S. 362, die gleichzeitig aber auch als „Gefahr“ ansehen, wenn nur Bestandsdaten übertragen werden sollten.

41 Siehe etwa die Dienste „DigiMe“ oder „MyData“ (behandelt in der Studie der Stiftung Datenschutz zum Thema „Neue Wege bei der Einwilligung im Datenschutz“, https://stiftungdatenschutz.org/themen/pims-studie/)

42 Auf die klärungsbedürftige Frage nach dem Dateneigentum verweisen unter anderem Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries, in der Studie der Stiftung Datenschutz „Praktische Umsetzung des Rechts auf Datenübertragbarkeit“, S. 208 ff.

43 Siehe etwa Lindhorst, Sanktionsdefizite im Datenschutzrecht (2009), S. 66 ff. zur informationellen Selbstbestimmung als Vermögensrecht; Unseld, Die Kommerzialisierung personenbezogener Daten (2010), S. 14 mit der Anmerkung, dass nur die zugrundeliegenden Datenträger kommerzialisiert werden, nicht aber die Person. Bezüglich dieser Daten (und Datenträger) müssten Rechte eingeräumt werden. Siehe auch Klüber, Persönlichkeitsschutz und Kommerzialisierung: die juristisch-ökonomischen Grundlagen des Schutzes der vermögenswerten Bestandteile des allgemeinen Persönlichkeitsrechts (2007), S. 82: Es werde erst im Rahmen einer rechtlichen Wertung entschieden, ob die Persönlichkeitsdetails der Allgemeinheit zugewiesen sind und damit öffentliche Güter darstellen oder ob der der Einzelne ein uneingeschränktes Verwertungsrecht an der eigenen Persönlichkeit hat. Weiter weist Klüber (aaO) auf die Rechtsprechung hin, nach welcher die vermögensrechtliche Seite des allgemeinen Persönlichkeitsrechts zwar anerkannt werde, ein kommerzieller Zuweisungsgehalt aber davon abhänge, dass zum einen die Erlaubnis zur Verwertung üblicherweise nur gegen Zahlung eines Entgelts erfolge und zum anderen die betroffene Person auch nutzungsbereit gewesen sei.

44 Artikel-29-Datenschutzgruppe, WP 242, S. 21.

45 Interoperabel bedeutet die Fähigkeit verschiedener und unterschiedlicher Organisationen zur Interaktion zum beiderseitigen Nutzen und im Interesse gemeinsamer Ziele, siehe hierzu Artikel-29-Datenschutzgruppe, WP 242, S. 20 mit Verweis auf Artikel 2 des Beschlusses Nr. 922/2009/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über Interoperabilitätslösungen für europäische öffentliche Verwaltungen (ISA) (ABl. L 260 vom3.10.2009, S. 20).

46 Herbst in: Kühling/Buchner, DS-GVO – BDSG, Artikel 20 DS-GVO Rn. 21.

47 Siehe den Hinweis der Artikel-29-Datenschutzgruppe auf die Existenz geeigneter Formate, WP 242, S. 20. Siehe auch Gerl/Pohl, The Right to data portability between legal possibilities and technical boundaries (in der Studie der Stiftung Datenschutz „Praktische Umsetzung des Rechts auf Datenübertragbarkeit“, S. 208 ff.), wobei diese Autoren in ihrer Stellungnahme die allgemeinen Bedingungen für ein entsprechendes Datenübertragungsformat anhand von unterschiedlichen Szenarien beschreiben und in der Übertragbarkeit an sich keine technische Hürde sehen.

48 Artikel-29-Datenschutzgruppe, WP 242, S. 21.

49 Artikel-29-Datenschutzgruppe, WP 242, S. 20 mit Verweis auf Erwägungsgrund 21 der Richtlinie 2013/37/EU.

50 Siehe zur Maschinenlesbarkeit auch BeckOK DatenSR/von Lewinski DS-GVO Art. 20 Rn. 74-75.

51 Artikel-29-Datenschutzgruppe, WP 242, S. 21.

52 Siehe Erwägungsgrund 55 des Vorschlags für eine VERORDNUNG DES

EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.01.2012, KOM(2012) 11 endgültig.

53 Artikel 18 Absatz 1 des Entwurfs des Vorschlags für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.01.2012, KOM(2012) 11 endgültig

54 Hennemann, Ping 01.17, S. 8.

55 Herbst in: Kühling/Buchner, DS-GVO – BDSG, Artikel 21 DS-GVO Rn. 27, auch mit Verweis auf Schürmann in Auernhammer Artikel 20 Rn. 30.

56 Herbst in: Kühling/Buchner, DS-GVO – BDSG, Artikel 21 DS-GVO Rn. 27.

57 Herbst in: Kühling/Buchner, DS-GVO – BDSG, Artikel 21 DS-GVO Rn. 35.

58 Siehe zu mehr Transparenz und Selbstdatenschutz auch die Studie der Stiftung Datenschutz „Neue Wege bei der Einwilligung im Datenschutz“, insbesondere auch zu „Personal Information Management Services“ (PIMS) https://stiftung-datenschutz.org/themen/pims-studie/

Philipp Schmidtke

Vereine unter der DSGVO

Wenn in Deutschland ein Hobby mehr als nur sporadisch ausgeübt wird, findet es meist in einem Verein statt. 44 % aller Deutschen sind in einem der 600.000 Vereine organisiert[1]. Die Bandbreite reicht hier von den Klassikern Sport-, Musik-, Kegelverein bis zum (vom Autor frequentierten) Debattierverein. Nun ist die Datenschutzgrundverordnung (DSGVO) da und viele Vereinsmeier fragen sich: Was tun? Der Landesbeauftragte für Datenschutz und Informationsfreiheit in Baden-Württemberg Dr. Stefan Brink kündigt an: „Vereine, die dokumentieren, dass sie sich Gedanken gemacht haben, werden von uns zunächst eher keine Probleme bekommen.“[2] Daraus lassen sich zwei Dinge schließen: Zum einen sollten Vereine sich aktiv um dieses Thema kümmern und zum anderen ist die Schonung nur zeitlich begrenzt. Grundsätzliche Informationen lassen sich zwar schon in einer Vielzahl von Ratgebern finden, unter anderem von Herr Dr. Brinks eigener[3] und von anderen Behörden.[4] Hier mangelt es jedoch häufig an dem notwendigen konkreten Praxisbezug, der den Datenschutz aus seiner rechtlichen Sphäre in operationalisierbare Handlungsanweisungen holt. Hier möchte dieser Aufsatz ansetzen und am Beispiel die abstrakten rechtlichen Problematiken darstellen. Das Problematische am Datenschutz ist jedoch, dass einem Laien des Datenschutzrechts der Blick für relevante Problemfelder meist fehlt und somit ggf. Hilfe von einem Sachkundigen gar nicht erst nötig erscheint. Darum möchte ich in diesem Text am Beispiel eines typischen Vereins die verschiedenen Tätigkeiten durchgehen und dabei typische Problemfelder beleuchten.

Als Beispiel dient der Debattierclub der Universität Münster e.V., einer der vielen Vereine des Hochschuldebattierens in Deutschland.[5] Er besteht aus rund 30 aktiven und über 100 passiven Mitgliedern. Der vierköpfige Vorstand verwaltet, mit weiteren Freiwilligen, die Clubaktivitäten. Diese bestehen neben der allgemeinen Mitgliederverwaltung aus wöchentlichen Trainings, Teilnahme an Turnieren und der eigenen Ausrichtung von Turnieren.

Die Grundlagen

Bevor die typischen praktischen Problemfelder beleuchtet werden, zunächst ein Überblick über die juristischen Konzepte, welche alle Problemfelder betreffen:

1. Sind die DSGVO und das BDSG überhaupt auf Vereine anwendbar?

Ja. Dies bedauert Dr. Stefan Brink: „Die DSGVO differenziert leider nur wenig zwischen multinationalen Unternehmen und nichtkommerziellen Vereinen.“[6] Gem. Art. 2 Abs. 1 DSGVO gilt die DSGVO für zumindest teilweise automatisierte oder nichtautomatisierte Verarbeitungen, die systematisch gespeichert werden sollen. Das bedeutet, dass Vereine, die zumindest die Namen der Mitglieder erfassen, schon im Geltungsbereich der Norm sind. Das Bundesdatenschutzgesetz (BDSG), die deutsche Ergänzung zur europäischen Verordnung, wendet die gleichen Kriterien in § 1 Abs. 1 S. 2 BDSG auf sehr weitreichend definierte „nichtöffentliche Stellen“ an, der Vereine unterfallen. Dabei kommt es nicht darauf an, ob der Verein ein eingetragener Verein ist oder nicht.[7]

2. Muss ein Verein ein Verzeichnis von Verarbeitungen führen?

Ja. Ein Verzeichnis von Verarbeitungen fasst alle Verarbeitungen eines Verantwortlichen so zusammen, dass eine Behörde bei der Kontrolle sofort eine vertiefte Übersicht über die datenschutzrechtlich relevanten Tätigkeiten eines Verantwortlichen hat. Es muss im Vorhinein erstellt werden, um im Bedarfsfall zügig vorgelegt werden zu können. Dem Verantwortlichen kann es helfen überflüssige Verarbeitungen oder zu umfangreiche Zugriffsrechte zu entdecken. Wenn personenbezogene Daten verarbeitet werden, greift Art. 30 DSGVO. Art. 30 DSGVO gilt für zunächst für jeden Verarbeiter. Die Ausnahme wegen weniger als 250 Mitarbeitern aus Art. 30 Abs. 5 DSGVO greift in den allermeisten Fällen nicht, da unter den

Rückausnahmen auch die regelmäßige Verarbeitung aufgezählt wird. Verarbeitung ist in Art. 4 Nr. 2 DSGVO definiert und beschreibt fast jede Tätigkeit im Zusammenhang mit Daten. Regelmäßig ist jede Verarbeitung, die in einem wiederkehrenden Rhythmus vorgenommen wird.

Der Debattierclub Münster verarbeitet nicht nur gelegentlich, sondern regelmäßig personenbezogene Daten: Dies geschieht schon alleine mit der vereinsrechtlich zwingend erforderlichen jährlichen Ladung zur Mitgliederversammlung, unabhängig davon, ob sie per E-Mail oder als Serienbrief versendet wird.

Ein Beispiel für ein Verzeichnis von Verarbeitungen wurde vom Bayerischen Landesamt für Datenschutz veröffentlicht[8] und nennt beispielhaft als Verarbeitungstätigkeiten: Lohnabrechnungen, Mitgliederverwaltung, Betrieb der Website des Sportvereins, Veröffentlichung von Fotos der Mitglieder und die Beitragsverwaltung. Diese und weitere Verarbeitungstätigkeiten werden unten im jeweiligen Abschnitt der Vereinstätigkeit näher beleuchtet. Zweck der Verarbeitung ist immer der in der Vereinssatzung festgelegte Vereinszweck, der aber für jeden einzelnen Verarbeitungsvorgang konkretisiert werden sollte.[9] Freilich können je nach konkreter Vereinstätigkeit weitere Verwaltungstätigkeiten hinzukommen bzw. einzelne beispielhaft aufgezählte Verwaltungstätigkeiten entfallen. Für den Debattierclub kämen ergänzend noch Trainingsorganisation und Archivierung von Trainingsmaterialien, Turnieranmeldungen, Turnierausrichtungen, Betrieb diverser E-Mail Verteiler und eine Spendenliste hinzu. Dafür fallen Lohnabrechnung und Beitragsverwaltung weg, da der Verein weder Mitgliedsbeiträge erhebt noch Angestellte hat.

3. Muss ein Verein eine Datenschutzfolgenabschätzung vornehmen?

Meistens nein. Eine Datenschutzfolgenabschätzung ist nur bei Verarbeitungstätigkeiten erforderlich, die voraussichtlich hohe Risiken für natürliche Personen bergen. Dies sollte für die allermeisten Vereine – und auch für den Debattierclub – nicht notwendig sein, da die Art und der Umfang der Datenverarbeitung sowie die eingesetzte Technologie (E-Mail-Verteiler, Vereins- und Buchhaltungssoftware) hier keine relevanten Risiken bergen.

4. Braucht ein Verein einen Datenschutzbeauftragten?

Ob ein Datenschutzbeauftragter zu bestellen ist, richtet sich nach Art. 37 Abs. 1 DSGVO und § 38 Abs. 1 S. 1 BDSG.

Nach § 37 Abs. 1 DSGVO ist dies der Fall, wenn die Kerntätigkeit des Verantwortlichen in einer Verarbeitung besteht, die nach Art, Umfang oder Zweck eine regelmäßige Überwachung von betroffenen Personen erforderlich macht oder wenn die Kerntätigkeit in der umfangreichen Verarbeitung von besonderen personenbezogenen Daten oder Daten über strafrechtliche Verurteilungen oder Straftaten besteht. Kerntätigkeit eines Vereins im Sinne des Art. 37 Abs. 1 b, c DSGVO ist die Haupttätigkeit eines Vereins, die ihn untrennbar prägt. Dazu gehören alle Vorgänge, die einen festen Bestandteil der Haupttätigkeit des Vereins darstellen, aber nicht das Kerngeschäft unterstützende Tätigkeiten.[10] Bei Vereinen bestimmt sich die Kerntätigkeit nach dem Vereinszweck. Ein Debattierclub veranstaltet Debatten zur Förderung der allgemeinen Streitkultur. Dass dabei Namen und Redeleistung aufgeschrieben werden, dient nur der Organisation der Debatten und der Ermöglichung von Feedback. Ebenso spielt ein Skatverein Skat und das Nachhalten, wer geben muss, dient dieser Tätigkeit.

Eine Pflicht zur Bestellung eines Datenschutzbeauftragten könnte sich somit nur aus § 38 Abs. 1 S. 1 BDSG ergeben, wenn mehr als 10 Personen sich ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Automatisierte Verarbeitung ist dabei jeder Einsatz von elektronischer Datenverarbeitung und deswegen kaum vermeidbar.

Dabei muss man sich vor Augen führen, wie viele Menschen tatsächlich für einen Verein tätig werden. Ständig beschäftigt ist schon jeder, der eine Tätigkeit normalerweise übernimmt, wenn sie anfällt.[11] Es muss auch keine Vollzeittätigkeit vorliegen und kein Beschäftigungsverhältnis. Mögliche Wechsel in der tatsächlichen Person hinter einer Rolle sind unbeachtlich, so dass ein neuer Vorstand nicht neue 4 Personen der Liste hinzufügt, sondern nur die alten Rollen neu besetzt werden.[12]

Auch selten ausgeführte Tätigkeiten gehören, wenn sie mit einer festen Position und Person bestimmt sind, dazu. Die meisten Vereine haben zwei Kassenprüfer, die am Ende jedes Geschäftsjahres den Bericht des Kassenwarts prüfen und dabei über Geldüberweisungen der Mitglieder natürlich auch mit personenbezogenen Daten in Kontakt kommen. Daneben können weitere durch Sonderaufgaben hinzukommen. Bei der Betrachtung der einzelnen Tätigkeiten werden diese Sonderfälle betrachtet.

Um die vielfältigen Aufgaben eines Vereines zu bewältigen, werden sie meist auf viele Schultern verteilt. Hier müssen nun genau die Vereinsorganisation durchgegangen und die einzelnen Rollen durchgezählt werden. Übersteigt diese Zahl 10 Personen, so ist ein Datenschutzbeauftragter mit Sachkenntnisnachweis zu bestellen.

5. Wie schnell müssen Vereine die Anforderungen der DSGVO und des BDSG umsetzen

Zügig. Die zwei Jahre Übergangsfrist sind vorbei und seit dem 25.05.2018 darf grundsätzlich mit Bußgeldern gerechnet werden. Zudem drohen Abmahnungen von Verbraucherverbänden auf Basis des § 3 UKlaG und u.U. von Wettbewerbern gemäß § 3a UWG.[13] Trotzdem geht für Vereine nach der Frist die datenschutzrechtliche Welt nicht sofort unter. Die Behörden werden nach den bisherigen Andeutungen nicht als erstes auf Vereine Jagd machen und werden auch bei gemeldeten Verstößen gnädiger sein, wenn erkennbar ist, dass der Verein sich um den Datenschutz bemüht hat. Die Verbraucherverbände können nur klagen, wenn die Datenschutzrechtsverletzung zugleich gegen Verbraucherschutz- oder AGB-Regeln verstößt. Verbraucherschutzrechte fallen in vielen Fällen als Grund weg, da Vereine keine Unternehmer im Sinne des § 14 BGB sind, da sie nicht gewerblich handeln. Die von einem Verein vor-

formulierten und für den wiederholten Gebrauch vorgesehenen Mitgliedsanträge sind zwar AGB, aber selten relevant genug für die Verbraucherschutzbehörden, um gegen in ihnen enthaltene Fehler vorzugehen.

Was folgt aus der DSGVO?

Die DSGVO ist ein guter Anlass für Vereine sich Gedanken zum Datenschutz zu machen. Eine Veränderung des bisherigen Systems in dem oftmals behaupteten Umfang fand nicht statt. Es ist nur leider so, dass bisher einfach die Datenschutzregelungen nicht umgesetzt wurden. Worauf ist dabei nun konkret zu achten? Jede Verarbeitung braucht einen Zweck und eine Rechtsgrundlage, die im Endeffekt auf einen der Fälle des Art. 6 DSGVO zurückverweist. Diese und weitere müssen in einem Verzeichnis von Verarbeitungen gemäß Art. 30 DSGVO festgehalten werden. Jedem Betroffenen stehen Rechte zu. Betroffenenrechte neben der Informationspflicht aus Art. 12 bis 14 DSGVO sind ein Auskunftsrecht gemäß Art. 15 DSGVO, ein Recht auf Berichtigung gemäß Art. 16 DSGVO, ein Recht auf Löschung gemäß Art. 17 DSGVO, ein Recht auf Einschränkung der Verarbeitung gemäß Art. 18 und ein Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO. Sofern in die Datenverarbeitung eingewilligt wurde, gibt es ein Widerspruchsrecht gemäß Art. 21 DSGVO.

Der Vereinsalltag

Der Vereinsalltag des Debattierclubs Münster besteht aus wöchentlichen, öffentlichen Debatten und regelmäßigen Trainings. Nicht nur Vereinsmitglieder, sondern jeder Interessierte kann teilnehmen. Bei einer Debatte werden zur Bewertung Jurierbögen verwendet, die die Vornamen der Redner enthalten sowie Notizen zu Inhalt und Form der Reden.

Eine Debatte ist ein guter Ausgangspunkt, um Schritt für Schritt eine Vorstellung zu bekommen, wie ein Verzeichnis von Verarbeitungen zu befüllen ist. Als erstes muss überhaupt eine Verarbeitung vorliegen. Verarbeitung ist gem. Art. 4 Nr. 2 DSGVO verkürzt gesagt jeder Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Personenbezogene Daten sind gem. Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen. Der Verein ist Verantwortlicher, da er Zweck und Mittel der Verarbeitung festlegt, indem er das Regelformat vorgibt und mit Jurierbögen Arbeitsmaterialien stellt. Bei den Debatten werden von Juroren die Redeinhalte mit dem Zweck Feedback geben zu können auf Jurierbögen notiert, dort also gespeichert. Die Speicherung erfolgt auch systematisch, weswegen die oben genannten Voraussetzungen für die Anwendbarkeit der DSGVO erfüllt sind, da die Blätter nach der Rednerreihenfolge sortiert und nummeriert werden. Die im studentischen Umfeld übliche Nutzung von Vornamen reicht aus, um durch den Kontext des Vereins eine Person zu bestimmen. Damit werden die Informationen einer identifizierbaren Person zugeordnet. Somit werden personenbezogene Daten in datenschutzrelevanter Weise verarbeitet.

Befüllung des Verzeichnisses von Verarbeitungstätigkeiten

Diese Verarbeitung „Debattenjurierung" muss in das Verzeichnis von Verarbeitungen eingetragen werden. Neben den Kontaktdaten des Verantwortlichen müssen die Zwecke der jeweiligen Verarbeitung, die Kategorien betroffener Personen und personenbezogener Daten, Kategorien etwaiger Empfänger der Daten, etwaige Auslandsübermittlungen, wenn möglich die vorgesehene Löschfrist und eine allgemeine Beschreibung der Technischen und Organisatorischen Maßnahmen angegeben werden. Zweck der Verarbeitung ist der Vereinszweck der Verbesserung der Debattenkultur und die Rechtsgrundlage ist dann Art. 6 Abs. 1 f) DSGVO[14], also die Wahrung der berechtigten Interessen des Verantwortlichen. Dies ist einer Einwilligung praktisch vorzuziehen, da dadurch zum einen organisatorischer Aufwand entfällt und zum anderen keine Möglichkeit des Widerrufs besteht, sondern nur die aus der DSGVO folgenden Betroffenenrechte. Die Kategorien der Betroffenen sind Mitglieder des Vereins und Gäste. Eine Übermittlung an Empfänger oder ins Ausland findet nicht statt.[15] Die Unterlagen sind zu vernichten, wenn der Zweck erfüllt ist, also die Redner ihr Feedback erhalten haben. Als organisatorische Maßnahme reicht eine regelmäßige Ermahnung (Löschkonzept) an die Juroren die Unterlagen zu vernichten.

Ein Juror zählt aber nicht zu den eine Bestellpflicht auslösenden Personen nach § 38 BDSG, da seine Verarbeitung nicht automatisiert, sondern rein händisch mit Stift und Papier erfolgt. Aus anderem Grund zum selben Ergebnis kommt das Bayerische Landesamt für Datenschutzaufsicht, das schon die „ständige" Beschäftigung bei Übungsleitern ablehnt.[16]

Informationspflichten

Natürlich muss eine betroffene Person über die Datenerhebung informiert werden. Da die Daten den Vereinen regelmäßig nur von den Betroffenen selbst bereitgestellt werden, richtet sich die Anforderungen an diese Informationen nach Art. 13 DSGVO.[17] Die Informationen sollen gemäß Art. 12 Abs. 1 S. 2 DSGVO schriftlich mitgeteilt werden, können aber auch in jeder anderen Form, unter anderem auch elektronisch, erteilt werden. Notwendig sind gemäß Art. 13 Abs. 1 DSGVO Name und Kontaktdaten des Verantwortlichen, Zweck und Rechtsgrundlage und das Interesse des Verarbeiters, wenn die Verarbeitung auf Art. 6 Abs. 1 f DSGVO beruht. Art. 13 Abs. 2 DSGVO ergänzt Informationspflichten über die Dauer der Speicherung, das Bestehen eines Auskunftsrechts, im Falle einer Einwilligung das Widerrufsrecht, das Beschwerderecht bei Aufsichtsbehörden, die Notwendigkeit der Bereitstellung der Daten und die Folgen einer Nichtbereitstellung und gegebenenfalls das Bestehen von automatisierten Entscheidungsprozessen.

Die Einordnung des von Art. 13 Abs. 2 DSGVO (und Art. 14 Abs. 2 DSGVO) ist noch nicht juristisch entschieden.[18] Während der Wortlaut „um eine faire und transparente Verarbeitung zu gewährleisten" eine Bedingung in dem jeweiligen zweiten Absatz zu enthalten scheint, geht die Art.-29-Gruppe von einer Gleichwertigkeit der Absätze aus.[19] Nach der Vorlage der Landesbeauftragten für den Datenschutz Niedersachsen zur Videoüberwachung ist eine verkürzte Information

über ausgewählte Teile von Absatz 1 und Absatz 2 ausreichend, wenn eine umfassende Erläuterung leicht erlangt werden kann.[20] Entsprechend wird teilweise ein kurzer Hinweis, gefolgt von einem Link, vorgeschlagen.[21] Solange dies noch nicht entschieden ist, ist dem vorsichtigen Verantwortlichen zu raten, immer alle Informationspflichten aus Absatz 1 und 2 zu befolgen.

Dabei muss aber keine Angst aufkommen, dass immer ein Papierberg mitgeführt werden muss. Für die Verarbeitung von personenbezogenen Daten von Gästen im Rahmen der Debatte könnte, sofern dies nicht auf einem Einsteigerabend ausführlich erklärt oder auf der Website erläutert worden ist, die mündliche Information lauten: „Ich als Juror des Debattierclub Münster (Verantwortlicher) werde heute Abend eure Reden mitschreiben um euch später Feedback geben zu können (Zweck). Dies machen wir, da wir ein Interesse im Sinne des Art. 6 Abs. 1 f DSGVO (Rechtsgrundlage) daran haben eure Debattierfähigkeiten zu verbessern (Interesse des Verarbeiters ist der Vereinszweck). Wenn ihr die Mitschrift nicht wünscht, kann ich die Debatte auch nicht für die anderen jurieren und kann euch deswegen leider nicht mitmachen lassen. (Folgen einer Nichtbereitstellung[22]). Ihr könnt gerne zu mir oder zum Vorstand kommen (Kontaktdaten), wenn ihr konkrete Fragen zur Verarbeitung habt (Hinweis auf das Recht auf Auskunft[23]). Wenn ihr mehr Feedback haben wollt, dann meldet euch bitte, bevor ich die Notizen heute Abend wegwerfe (Speicherdauer). Ihr könnt euch auch an die Landesdatenschutzbeauftragte des Landes NRW wenden, wenn ihr euch beschweren wollt."

Diese Informationspflicht mag unverhältnismäßig klingen, ist aber vom Gesetz ohne Ausnahmetatbestand vorgesehen. Art. 13 Abs. 4 DSGVO erlässt die Informationspflichten nur, wenn dem Betroffenen die Informationen schon bekannt sind, da er z. B. schon letzte Woche informiert wurde. Nur Art. 14 Abs. 5 lit. b DSGVO erlässt Informationspflichten aufgrund von übermäßigem Aufwand. Der dahinterstehende Gedanke ist, dass niemand durch die Mitschriften abgeschreckt wird, da er nicht sicher ist, wie diese verwendet werden. Natürlich ist es jedem Verantwortlichen überlassen, ob er hier dem Gesetz folgen möchte oder sich dem Risiko aussetzt den Rechtsverstoß im Falle einer (eher unwahrscheinlichen) Beschwerde erst gegenüber einer Datenschutzaufsichtsbehörde und danach möglicherweise vor Gericht mit der Unverhältnismäßigkeit zu begründen.

Löschfrist

Warum werden die Notizen am Abend entsorgt? Das Recht Daten zu speichern endet immer dann, wenn die Rechtsgrundlage wegfällt. Bei Art. 6 Abs. 1 f) DSGVO ist dies das Ende eines berechtigten Interesses. Über den Debattenabend hinaus helfen Juriernotizen nicht mehr die Streitkultur zu verbessern.

Mitgliederverwaltung

Die Vereins- und Mitgliederverwaltung wird von vier Vorstandsmitgliedern vorgenommen, die alle mit personenbezogenen Daten durch E-Mail-Listen für regelmäßige Informationen oder durch Mitgliederkarteien zu tun haben. Jede dieser Tätigkeiten ist als ein Verarbeitungsvorgang ins Verzeichnis von Verarbeitungen aufzunehmen. Wünschenswert ist, wenn ein Verein seinen Vorstand so geregelt hat, dass jedes Vorstandsmitglied nur auf die für die zugeordneten Tätigkeiten notwendigen Daten zugreifen kann, da diese organisatorische Maßnahme die Gefahr einer Datenpanne reduziert und zugleich dem Gebot der Datensparsamkeit folgt. Zum Beispiel hat in den meisten Vereinen nur der Kassenwart Zugriff auf das Vereinskonto und die damit verbundenen Kontodaten der Mitglieder.

Neben den wöchentlichen Debatten finden regelmäßig Trainings statt, die von einer Reihe erfahreneren Mitglieder abwechselnd und freiwillig ohne Gegenleistung gehalten werden. Eine E-Mail-Liste der Anwesenden zur Versendung der Vortragsinhalte würde bei der Verwendung eine automatisierte Verarbeitung darstellen. Die Trainer sind aber nicht dauerhaft, sondern nur für diesen Abend mit der Versendung von E-Mails an die Teilnehmerliste betraut und deswegen nicht im Sinne von § 38 BDSG mitzuzählen.[24]

Ein nicht dem Vorstand angehörender Trainingsleiter, der aus dem Pool der möglichen Trainer einzelne auswählt und die Termine in seinem Handykalender zur Koordinierung speichert, ist zu den mit der Verarbeitung Beschäftigten zu zählen und der Vorgang ist natürlich ins Verzeichnis von Verarbeitungen aufzunehmen.

Informationspflichten

Ganz ähnlich zu der oben vorgeschlagenen Formulierung lautet die einem neuen Mitglied schriftlich übergebene Information, die alle Verarbeitungen im Rahmen der Mitgliederverwaltung umfassen soll: „Wir, der Debattierclub Münster e.V., benötigen deinen Namen und deine Adresse, um mit dir Kontakt zu halten, dich zu unserer Mitgliederversammlung einzuladen und dir Trainingsmaterialien zukommen zu lassen, solange du Mitglied bist. Wir werden, wenn du an Debatten teilnimmst, deine Redeinhalte von Juroren notieren lassen, damit sie dir Feedback gegen können. Die Datenverarbeitung erfolgt gemäß Art. 6 Abs.1 f) DSGVO, um dich am Vereinsgeschehen teilhaben zu lassen."

Bei Mitgliedsbeiträgen wäre noch Folgendes anzufügen: „Damit du deiner Verpflichtung zur Zahlung eines Mitgliedsbeitrag nachkommen kannst, werden wir darüber Buch führen, ob du ihn schon gezahlt hast und dich gegebenenfalls kontaktieren. Du kannst uns aber auch das Mandat erteilen den Betrag von deinem Konto einzuziehen. Dann werden wir zusätzlich deine Kontodaten speichern und sie an unsere Bank zum Zweck der Einziehung weitergeben. Diese Verarbeitung erfolgt gemäß Art. 6 Abs. 1 b) DSGVO. Wir werden deine Daten löschen, sobald du aus dem Verein austrittst und deine Daten nicht mehr aufgrund von gesetzlichen Pflichten benötigt werden."

Die Löschpflicht tritt hier mit der Beendigung der Mitgliedschaft bei Austritt ein. Wer nicht mehr Mitglied ist, braucht keine E-Mails vom Vereinsvorstand und dessen Kontodaten werden für Abbuchungen nicht mehr benötigt.[25] Wer weiterhin informiert werden will, z. B. als Alumnus, muss in die Datenverarbeitung einwilligen.

Verwaltungssoftware

Sofern Teile der Vereinsverwaltung über eine Software ablaufen, ist dies unproblematisch, bis über diese Software ein weiteres Unternehmen Zugriff auf personenbezogene Daten bekommt. Dies ist beispielsweise bei „Software as a Service"-Angeboten oder bei der Verwendung von Cloudspeichern der Fall. Da die Übermittlung an ein unbeteiligtes Unternehmen selten nach Art. 6 DSGVO rechtfertigbar ist, muss dieser Dienstleister durch einen Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO zum Verantwortlichen hinzugezogen werden. Für diesen Fall gibt es ein Muster aus Baden-Württemberg.[26] Ansonsten sollten kommerzielle Anbieter auch eine eigene Vorlage haben, die sie ihren Kunden anbieten können.

Kommunikation

Eine der wichtigsten Aufgaben eines Vereins ist die Kommunikation mit den Mitgliedern und der Öffentlichkeit, da nur so neue Mitglieder gewonnen werden können. Dies erfolgt heutzutage aber nicht mehr nur durch Ansagen am Vereinsabend oder Telefonketten, sondern zumeist wird eine volle Breitseite digitaler Dienste verwendet. Die Mitgliederkommunikation erfolgt beim Debattierclub Münster über eine E-Mail-Liste, geschieht aber parallel auch per Facebook. Zudem werden Nichtmitglieder durch eine Website und eine Facebook-Seite über Neuigkeiten informiert.

E-Mail-Liste

Die Aufnahme in den E-Mail-Verteiler erfolgt entweder durch Mitgliedschaft (s.o., Mitgliederverwaltung) oder auf Grundlage einer Anfrage durch eine Person, die (noch) nicht Vereinsmitglied ist. Im letzteren Fall ist die darauffolgende Verarbeitung in Form des Auf-die-Verteilerliste-schreibens auf der Basis der Einwilligung gemäß Art. 6 Abs. 1 a) DSGVO gerechtfertigt.

Um der Nachweispflicht aus Art. 7 Abs. 1 DSGVO nachzukommen, muss die Einwilligung schriftlich erfolgen. Ausnahmsweise ist auch der Zeugenbeweis zulässig. Dieser könnte im Streit Aussage gegen Aussage obsiegen, wenn es nur darauf ankommt, ob jemand seine E-Mail-Adresse freiwillig herausgegeben hat, um Informationen zu erhalten.

Eine nicht mit anderen Erklärungen verbundene Einwilligung muss nicht die Anforderungen an eine verständliche, leicht zugängliche Form nach Art. 7 Abs. 2 DSGVO erfüllen. Dies ist aber auch denklogisch, da sie zumeist ein einfacher Zettel ist, auf dem sich jemand eintragen kann, der E-Mails bekommen möchte, dessen Bedeutung offensichtlich sein sollte. Dabei sind natürlich die Informationspflichten nach Art. 13 DSGVO zu beachten.

Website

Die datenschutzrechtlich einfachsten Websites sind solche ohne Tracker, Add-Ins oder Social-Media-Widgets. Und die meisten Vereine benötigen diese auch nicht, um über ihre Tätigkeit zu informieren. Jedes Tool sollte einen Zweck haben und dieser Zweck deckt sich in diesen Fällen oft mit der Beschreibung der Verarbeitung für das Verarbeitungsverzeichnis. Natürlich muss dann auch über diese Verarbeitung informiert werden. Dafür sollte ein Menüpunkt „Datenschutz" von jedem Teil der Website aus erreichbar sein, der zur einer Informationsseite führt.[27] Die Website des Debattierclubs ist bei einem bekannten Bloganbieter gehostet und verwendet Google Analytics. Zum Glück hat dieser Bloganbieter gerade DSGVO-konforme Einstellungen eingerichtet, so dass zumindest die Betroffenenrechte leichter zu erfüllen sind.[28] Die leichte Umsetzbarkeit dieser Rechte wird für viele an rechtliche Laien gerichteten Angebote in Zukunft immer öfter als Service neben dem Hauptprodukt angeboten werden, da es den Bedienkomfort erhöht, auf dessen Basis solche Angebote konkurrieren. Es bleibt die Pflicht zur rechtskonformen Anwendung. Diese sollte aber nicht zu schwer sein, da nach Erfahrung des Autors Vereine auch ohne rechtliche Pflicht gerne die Wünsche von einzelnen Mitgliedern oder vereinsfremden Personen beachten.

Es sollte festgestellt werden, ob ein Analysetool wie z. B. Google Analytics tatsächlich sinnvoll verwendet wird. Ist dies nicht der Fall, sollte es entfernt werden. Ansonsten ist die Abwägung nach Art. 6 Abs.1 f) DSGVO zu treffen, ob das Interesse des Vereins an der statistischen Auswertung das Interesse der Betroffenen überwiegt.

Wenn es wirklich ein Facebook-Like-Button sein soll, dann in der Variante, die nicht sofort, sondern erst durch bewusste Aktivierung Daten überträgt.[29]

Die Datenschutzerklärung für die Website ist bei juristisch unterbesetzten Vereinen am besten aus dem ausführlichem Muster von Prof. Hoeren der Universität Münster zusammenzustellen, das die häufigsten Websitekonfigurationen abdeckt.[30]

Soziale Medien

Für eine moderne Vereinsarbeit werden aber auch weitere internetbasierte Werkzeuge genutzt. Die Verwendung ist für die Erfüllung der Vereinszwecke nicht zwingend notwendig und deswegen nicht mit Art. 6 Abs. 1 f) DSGVO begründbar. Notwendig für diese zusätzliche Verarbeitung ist eine Einwilligung, die sich am Muster der Orientierungshilfe der Baden-Württemberger [31] orientieren könnte.

Facebook*

Da die Verantwortlichkeiten bei der Nutzung von Facebook schwer zu überblicken sind[32] und dies zu verstehen die notwendigen Kompetenzen eines Vereinsvorstandes überschreitet, ist dem Laien zu raten, sich erst einmal auf die Aussage des Datengiganten zu verlassen, dass es selbst überwiegend Verantwortlicher für die Datenverarbeitung ist und nur bei kostenpflichtigen Werbemaßnahmen eine Auftragsverarbeitung vorliegt.[33] Letztere liegen bei einem Verein üblicherweise nicht vor. Es ist nur noch zu prüfen, ob Facebook alleine oder gemeinsam Verantwortlicher für die Verarbeitungsvorgänge auf der ihrer Seite ist. Damit sind „Likes" für eine Vereinsseite auf Facebook wohl abgedeckt, da ein Verein hier weder über Zweck noch Art der Verarbeitung Kontrolle hat und kein Verantwortlicher ist. Gemeinsame Verarbeitung von mehreren Verantwortlichen nach Art. 26 DSGVO liegt vor, wenn der Verein auf Facebook personenbezogene Daten teilt, da er dann entscheidet, dass diese Daten via Facebook veröffentlicht werden sollen. Es ist ratsam dafür eine

Einwilligung einzuholen und im Rahmen der Informationspflichten auf die Nutzung von Facebook und deren Verhaltensweisen ausdrücklich hinzuweisen. Sollte es darüber hinaus zu einem Datenschutzvorfall kommen ist im Rahmen einer gesamtschuldnerischen Haftung[34] wohl die Verantwortung weit überwiegend bei Facebook und seinem überlegenen Verständnis der Datenstrukturen zu suchen.

Whatsapp

Die Verwendung der üblichen Funktionen von Whatsapp ist für juristische Personen nach den AGB von Whatsapp nicht gestattet. Es müsste ein kostenpflichtiger Unternehmensaccount erstellt werden. Somit sollte ein Verein es sich gut überlegen, ob er Whatsapp tatsächlich nutzen möchte. Unabhängig vom Verein können natürlich einzelne Vereinsmitglieder sich in einer Whatsapp-Gruppe zusammenschließen und über den Verein und Vereinsaktivitäten schreiben.

Veröffentlichungen von Fotos

Ein besonders dramatisierter[35] Fall ist die Frage nach Fotografien. Diese werden typischerweise zu verschiedensten Anlässen im Verein gemacht. Die fotografische Dokumentation ist natürlich ein Interesse der Verantwortlichen im Sinne des Art. 6 f) DSGVO. Nach Ansicht des Bundesinnenministeriums stimmt das Interesse mit der Informations- und Meinungsfreiheit überein.[36] Die Veröffentlichung von Fotografien wurde zuvor über das Kunsturhebergesetz (KUG) geregelt. Obwohl das Gesetz von 1907 ist, gilt es weiterhin. Durch Art. 85 Abs. 1 DSGVO wurde eine Öffnungsklausel für Meinungsäußerung und Informationsfreiheit geschaffen, die durch das KUG ergänzt wird. Somit ändert sich durch die DSGVO nichts Wesentliches. Der Debattierclub Münster fragt aber aus Höflichkeit schon seit Jahren, ob jemand nicht abgebildet werden will und weist Fotografen an es zu vermeiden diese Personen in Einzel- oder Gruppenbildern abzulichten.

Vereinsmitglieder lassen sich leicht über die Fotografien auf Vereinsveranstaltungen gemäß Art. 13, 14 DSGVO informieren. Gegenüber unbekannten Gästen sind die Informationspflichten laut eines internen Vermerks der Hamburger Behörde wegen Art. 11 DSGVO nicht zu erfüllen, da für die Dokumentation der Veranstaltung die Identifikation der Betroffenen nicht notwendig ist oder zumindest gemäß Art. 14 Abs. 5 lit. b Var. 1 und 2 DSGVO das Informieren zu aufwändig wäre.[37]

Turnierausrichtung

Vereine führen nicht nur regelmäßige Veranstaltungen für ihre Mitglieder durch, sondern auch Events für Gäste. Dafür müssen sich Gäste anmelden, die dann mit Unterkunft, Essen und einem Turnier versorgt werden.

Anmeldung

Bei der Turnierausrichtung müssen Daten aufgenommen werden, um den Ablauf der Veranstaltung zu ermöglichen. Die Verarbeitungsvorgänge müssen dann natürlich in das Verzeichnis von Verarbeitungen aufgenommen werden und die Informationspflichten aus Art. 13 oder Art. 14 DSGVO sind zu beachten. Da oftmals auch Nahrungsunverträglichkeiten der Angemeldeten bei der Bewirtung relevant sind, kommt es zur Verarbeitung von Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO und deswegen gilt dafür Art. 9 DSGVO, der aber in Abs. 2 lit a DSGVO auch eine Einwilligung als Rechtsgrundlage vorsieht. Diese kann so ausgestaltet werden, dass über die Verarbeitung informiert wird. „Wenn du möchtest, dass wir auf etwaige Besonderheiten bei deiner Ernährung achten sollen, so gibt sie bitte hier an.“ Daneben sind bei der Anmeldung die üblichen Informationen nach Art. 13 DSGVO bereitzustellen. Um Komplikationen zu vermeiden, sollte die Anmeldung mit personenbezogenen Daten immer durch die Betroffenen selbst stattfinden, während ihr Verein nur die nicht personenbezogenen Rahmenvereinbarungen trifft.

Sollte ein Verein seine Mitglieder gesammelt anmelden, liegt hier eine rechtfertigungsbedürftige Verarbeitung in Form einer Übermittlung von Daten an Dritte vor. Dies muss im Verzeichnis von Verarbeitungen und den Informationspflichten bei der internen Anmeldung (Zeitpunkt der Erhebung) beachtet werden. Rechtsgrundlage könnte Art. 6 Abs. 1 b) DSGVO sein, wenn der Verein es als kostenlose Dienstleistung seinerseits ansieht die Reise zu organisieren, denn auch ein mündlicher Vertrag ist eine gültige Rechtsgrundlage.

Das Empfangen ist eine eigenständige Verarbeitung des Ausrichters und muss deswegen wie eine normale Erhebung behandelt werden, nur dass die Informationspflichten sich nach Art. 14 DSGVO richten, da die Daten nicht mehr vom Betroffenen selbst erhoben wurden.

Ergebnisse

Ergebnisse von Turnieren dürfen veröffentlich werden, wenn zuvor über diese Veröffentlichung gemäß den Pflichten aus Art. 13 DSGVO informiert wurde.[38] Grundsätzlich hat die Öffentlichkeit ein Interesse an den Ergebnissen von Wettkämpfen aller Art. Dies kann ein berechtigtes Interesse an der Veröffentlichung gemäß Art. 6 Abs. 1 f) DSGVO darstellen, insbesondere wenn eine Anonymisierung angeboten wurde und somit möglichen Bedenken entgegengekommen ist. Zudem steht einem Betroffenem das Recht auf Widerspruch aus Art. 21 DSGVO zu, so dass Einzelfälle zusätzlich zwischen Informationserhebung und Veröffentlichung nachbewertet werden können. Die Dauer einer Veröffentlichung sollte aber zeitlich begrenzt werden. Es besteht weniger Interesse an der langfristigen Nachvollziehbarkeit, wer wann Vorletzter geworden ist, als bei den FinalistInnnen.

Zusammenfassung

Die Änderungen der DSGVO greifen nicht tief in die Abläufe von Vereinen ein, da die allermeisten Tätigkeiten zulässig sind. Sie verlangen nur erheblich ausführlichere Dokumentation der Vereinsvorgänge in Form eines Verfahrensverzeichnisses und von Informationspflichten. Vereine sollten diese Herausforderung nicht als eine Belastung, sondern als Anlass zur kritischen Kontrolle von eingefahrenen Strukturen sehen. Ein Verein mit Übersicht über seine Datenverläufe hat ein tieferes Selbstverständnis.

1 http://www.stiftungfuerzukunftsfragen.de/de/newsletter-forschung-aktuell/254.html

2 https://www.t-online.de/digital/id_83709562/tid_amp/datenschutz-grundverordnung-datenschuetzer-stefan-brink-erklaert-wie-hart-es-ab-25-mai-wird.html

3 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-f%C3%BCr-Vereine.pdf

4 https://datenschutz.saarland.de/themen/vereine/datenschutz-im-verein/

https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Datenschutz_im_Verein__DS-GVO__-_Kompakt.pdf

https://www.lda.bayern.de/media/muster_1_verein.pdf

5 http://www.vdch.de/debattieren/

6 https://www.t-online.de/digital/id_83709562/tid_amp/datenschutz-grundverordnung-datenschuetzer-stefan-brink-erklaert-wie-hart-es-ab-25-mai-wird.html

7 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf S.5

8 https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf Allgemeineres Muster: https://www.lfd.niedersachsen.de/themen/wirtschaft/verfahrensverzeicnis_und_verfahrensregister_nach_bdsg/verfahrensregister-und-verfahrensbeschreibung-fuer-den-nicht-oeffentlichen-bereich-56247.html

9 Orientierungshilfe des BayLDA, S. 7

10 https://www.lda.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf S.1

11 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-f%C3%BCr-Vereine.pdf S.6

12 Kühling/Sackmann BDSG § 38 Rn. 10

13 Es ist umstritten, ob Datenschutzrecht überhaupt eine Marktverhaltensregel ist und somit Abmahnungen von Wettbewerbern möglich sind. Dies wird durch die nun zu erwartenden Klagen gerichtlich geklärt. Allgemein zu Abmahnern: http://www.rechtzweinull.de/archives/2579-abmahnwellen-wegen-dsgvo-verstoessen-dagegen-spricht-und-wie-man-abmahnungen-gegebenenfalls-abwehren-kann.html

Spezifisch zum Streit: https://loeffel-abrar.com/newsblog/sind-verstoesse-gegen-die-datenschutz-grundverordnung-wettbewerbswidrig/

Nicht hübsch, aber kurz und bündig: https://www.evernote.com/shard/s344/sh/aad60f3b-3c66-411c-a354-cf08488ebc84/b6f7beaf2c0f8563

14 Dies gilt für offene Veranstaltungen. Für Vereinsmitglieder wäre Art. 6 Abs. 1 b) DSGVO mit dem Vereinszweck als Vertragsinhalt gemäß Satzung spezieller.

15 Wichtig ist, dass dies tatsächlich nicht der Fall ist. Bei einer Debatte, bei der die Jurierbögen nur in Papierform verwendet werden, ist dies unproblematisch. Werden aber Daten digital erhoben und dann bei einschlägigen Cloud-Dienstleistern gespeichert, so muss dies hier vermerkt werden. Im Übrigen ergeben sich daraus umfangreiche weitere Verpflichtungen.

16 https://www.lda.bayern.de/media/muster_1_verein.pdf S.2

17 Soweit andere Quellen für die Daten bestehen, ist Art. 14 DSGVO zu beachten.

18 Ausführlicher: https://www.datenschutzbeauftragter-info.de/erfuellung-der-informationspflichten-ist-ein-medienbruch-zulaessig/

19 WP 260 rev.01 Rn. 23, zu finden unter https://datenschutz-hamburg.de/assets/pdf/wp260rev01_en.pdf

20 https://www.lfd.niedersachsen.de/download/123755/Transparenzanforderungen_und_Hinweisbeschilderung_bei_Videoueberwachung.pdf

21 aufbauend auf WP 260 rev.01 Rn. 35ff https://www.datenschutz-guru.de/erfullung-der-dsgvo-informationspflichten-die-link-losung/

22 Ist die Tätigkeit auch ohne die Verarbeitung möglich, so darf die Verarbeitung nicht an die Teilnahme gekoppelt werden.

23 Die Rechte auf Berichtigung, Löschung, Einschränkung und Widerspruch sind nicht zu nennen, da sie dem Betroffenen im Ablauf der Debatte nicht zustehen und auch nicht danach entstehen, da eine Löschung sofort folgt.

24 https://www.lda.bayern.de/media/muster_1_verein.pdf s.2

25 https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/dsgvo---kurzpapiere-155196.html.

26 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-f%C3%BCr-Vereine.pdf

27 So zumindest § 13 TMG, dessen Schicksal mit dem Wegfall der Datenschutzrichtlinie und der noch ausstehenden E-Privacy Verordnung offen ist.

28 www.heise.de/amp/meldung/DSGVO-WordPress-mit-neuen-Datenschutzfunktionen-4052091.html

29 https://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html

30 https://www.uni-muenster.de/Jura.itm/hoeren/itm/wp-content/uploads/Musterdatenschutzerk%C3%A4rung-nach-der-DSGVO.docx

31 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-f%C3%BCr-Vereine.pdf S. 16

32 Ausführlich dazu: Barbara Elisabeth Schunicht in: „Informationelle Selbstbestimmung in sozialen Netzwerken: Mehrseitige Rechtsbeziehungen und arbeitsteilige Verantwortungsstrukturen als Herausforderung für das europäisierte Datenschutzrecht“. Frei zugänglich unter https://intr2dok.vifa-recht.de/receive/mir_mods_00003131

33 https://www.facebook.com/business/gdpr#Facebook-als-Datenverantwortlicher-vs.-Auftragsverarbeiter

34 Schunicht aaO S. 347

35 https://www.cr-online.de/blog/2018/03/09/das-ende-der-freien-veroeffentlichung-von-personenbildnissen-fuer-die-meisten-von-uns/

https://www.telemedicus.info/article/3265-Datenschutz-Grundverordnung-Das-Ende-der-modernen-Presse-und-OEffentlichkeitsarbeit-wie-wir-sie-kennen.html

36 https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/it-digitalpolitik/datenschutz/datenschutzgrundvo-liste.html

37 https://www.filmverband-suedwest.de/wp-content/uploads/2018/05/Vermerk_DSGVO.pdf

38 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf S.27/28

* Anmerkung des Redakteurs: Der Artikel wurde vor dem Urteil des EuGH vom 05. Juni 2018 zu Facebook-Fanpages geschrieben und berücksichtigt die Erkenntnisse aus diesem Urteil deswegen noch nicht.

Robert Zieske

Der Betriebsrat als datenschutzrechtlicher „Verantwortlicher“ im Sinne der DSGVO

Bereits unter dem bisherigen Regelungsregime des BDSG a.F. war strittig, ob selbstständige Organisationseinheiten innerhalb eines Unternehmens datenschutzrechtlich als „verantwortliche Stelle“ zu qualifizieren sind. Konkret stellt sich daher bei Unternehmen mit einem Betriebsrat die Frage, ob dieser selbst verantwortliche Stelle im datenschutzrechtlichen Sinne sein kann und daran anschließend, ob der betriebliche Datenschutzbeauftragte seine Kontrollaufgaben auch gegenüber dem Betriebsrat wahrnehmen kann. Im Vorfeld des Geltungsbeginns der DSGVO entflammte diese Diskussion mit neuer Intensität auf.[1] Daher ist zu klären, inwieweit diese Fragestellungen nunmehr im Kontext der neuen Regelungen des Datenschutzes rechtlich anders zu bewerten sind.

1. Der Betriebsrat als „verantwortliche Stelle“ im BDSG a.F.

Anknüpfungspunkt der datenschutzrechtlichen Verantwortlichkeit ist der Begriff der „verantwortlichen Stelle“ nach § 3 Abs. 7 BDSG a.F. „Verantwortliche Stelle“ in diesem Sinne ist „[...] jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt[...]“. Verantwortliche Stelle ist damit jedenfalls das Unternehmen selbst. Strittig war und ist weiterhin die Frage, ob der Betriebsrat als unabhängiges Organ und selbstständige Einheit innerhalb eines Unternehmens unter diese Definition subsumiert werden kann. Nach wohl herrschender Meinung[2] und nach ständiger Rechtsprechung[3] wurde er bisher nicht als eigenständige verantwortliche Stelle in diesem Sinne angesehen. Der Betriebsrat ist damit auch nicht Dritter im Sinne des § 3 Abs. 4 Nr. 3 BDSG a.F., sondern Teil der verantwortlichen Stelle selbst. Die datenschutzrechtliche Verantwortung trägt damit das Unternehmen. Dieses Ergebnis steht auch im Einklang mit der Datenschutz-Richtlinie 95/46/EG. Die Artikel-29-Gruppe hat sich im WP 169[4] dahingehend positioniert, dass sich für Bestimmung der verantwortlichen Stelle soweit wie möglich an der im öffentlichen und im privaten Sektor üblichen Rechtspraxis (z. B. Zivil -, Verwaltungs- und Strafrecht) zu orientieren sei.[5]

2. Der Betriebsrat als „Verantwortlicher“ im Sinne der DSGVO

Aus der „verantwortlichen Stelle“ wird mit der seit 25. Mai 2018 geltenden DSGVO der „Verantwortliche“. Mit dieser Änderung wird allerdings nicht nur eine terminologische Anpassung vorgenommen, sondern auch die Definition des Verantwortlichen erweitert. Nach Art. 4 Nr. 7 DSGVO ist „Verantwortlicher“ im Sinne der Verordnung „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Fraglich ist, ob der Betriebsrat unter die neue Definition subsumiert werden kann.

a) Der Betriebsrat als „Verantwortlicher“

Zentrales Kriterium zur Bestimmung des Verantwortlichen nach Art. 4 Nr. 7 DSGVO ist die Entscheidungshoheit über die Zwecke und die Mittel der Verarbeitung personenbezogener Daten.[6] Eine Ausnahme für den Fall, dass eine selbstständige Einheit als Teil eines Unternehmens agiert, existiert dabei nicht.[7] Konkretisiert wird die Definition allerdings durch Art. 29 DSGVO, der darauf abstellt, ob eine weisungsgebundene Verarbeitung der personenbezogenen Daten erfolgt oder nicht. Im letztgenannten Fall entscheidet die Organisationseinheit selbstständig über den Zweck und die Mittel der Datenverarbeitung und wird dann im Sinne des Art. 4 Nr. 7 DSGVO letztlich selbst verantwortliche Stelle – verbunden mit allen Rechten und Pflichten.[8] Übertragen auf den Betriebsrat bedeutet dies, dass dieser nur dann nicht selbst verantwortliche Stelle sein kann, wenn er sich bei der Verarbeitung der personenbezogenen Daten in seiner Zuständigkeit an die Weisungen des Unternehmens hält. Die §§ 78, 80 Abs. 2 S. 2 BetrVG stehen einer solchen Weisungsgebundenheit allerdings entgegen. Daher wird nach Caumanns die Voraussetzung als Verantwortlicher qua Definition gerade auch durch einzelne Organe oder Stellen, einschließlich des Betriebsrats, erfüllt.[9] Eine „Gesellschaftsrechtsakzessorietät“[10] besteht mithin gerade nicht.

b) Der Betriebsrat als Teil des Verantwortlichen

Allerdings ist zu berücksichtigen, dass zur Bestimmung des Verantwortlichen gem. Art. 4 Nr. 7 DSGVO die Entscheidung über Zwecke und Mittel der Verarbeitung nur ein und nicht alleiniges Merkmal ist. Darüber hinaus ist es auch erforderlich, richtiger Adressat der Verantwortlichkeitszuweisung im Sinne von Art. 4 Nr. 7 DSGVO zu sein.[11] Per Definition kann nur eine „juristische Person, Behörde, Einrichtung oder andere Stelle“ Adressat der Verantwortlichkeitszuweisung sein. Hierbei handelt es sich um eine alternative Aufzählung. Dem Wortlaut entsprechend ist damit ausgeschlossen, dass Verantwortlicher eine juristische Person sein kann und zugleich auch deren Einheiten und Organe.[12]

Unstreitig ist darüber hinaus, dass der Betriebsrat nicht weisungsgebunden handelt, da dies seiner Funktion und Stellung zuwiderliefe. Ein Rückgriff auf Art. 29 DSGVO führt aber gerade nicht

automatisch dazu, dass der Betriebsrat als Verantwortlicher zu qualifizieren ist. In Fällen, in denen eine dem Verantwortlichen unterstellte Person personenbezogene Daten nicht nach dessen Weisung verarbeitet, weil sie nach Unionsrecht oder nationalen Rechtsvorschriften zur Verarbeitung verpflichtet ist, wird sie gerade nicht selbst zum Verantwortlichen (Art. 29 2. HS). Wenn sie zum Verantwortlichen würde, stünde dies der gesetzgeberischen Intention entgegen, dass alleine die Erfüllung einer gesetzlichen Verpflichtung durch eine dem Verantwortlichen unterstellte Person kein Aufschwingen zum eigenständigen Verantwortlichen bedeuten muss. Sonst könnte bspw. auch die Personalabteilung eines Unternehmens als Verantwortlicher in diesem Sinne zu qualifizieren sein. Damit gäbe es innerhalb großer Unternehmen eine Vielzahl an Verantwortlichen.

Die rechtliche Verpflichtung zur Datenverarbeitung, der der Betriebsrat unterliegt, ergibt sich aus den Aufgaben des Betriebsrates nach dem BetrVG. Neben den allgemeinen Aufgaben des Betriebsrates nach § 80 BetrVG sieht § 99 Abs. 1 BetrVG in Unternehmen mit in der Regel mehr als zwanzig wahlberechtigten Arbeitnehmern bspw. vor, dass der Arbeitgeber den Betriebsrat vor jeder Einstellung, Eingruppierung, Umgruppierung und Versetzung zu unterrichten, ihm die erforderlichen Bewerbungsunterlagen vorzulegen und Auskunft über die Person der Beteiligten zu geben hat. Er hat dem Betriebsrat außerdem unter Vorlage der erforderlichen Unterlagen Auskunft über die Auswirkungen der geplanten Maßnahme zu geben und die Zustimmung des Betriebsrats zu der geplanten Maßnahme einzuholen. Bei Einstellungen und Versetzungen hat der Arbeitgeber insbesondere den in Aussicht genommenen Arbeitsplatz und die vorgesehene Eingruppierung mitzuteilen. Bezüglich der Aufgabenzuweisung im BetrVG ist gem. § 1 Abs. 2 S. 1 BDSG n.F. dann im Einzelfall zu prüfen, ob sich die Rechtsgrundlage für die Datenverarbeitung des Betriebsrates unmittelbar aus der entsprechenden Vorschrift des BetrVG direkt ergibt oder jedenfalls zur Erfüllung der im BetrVG genannten Aufgaben im Zusammenspiel mit § 26 Abs. 1 BDSG n.F. bewertet werden muss.[13]

Eine Ausnahme gilt dann, wenn der Betriebsrat personenbezogene Daten verarbeitet, die nicht zur Aufgabenerfüllung nach dem BetrVG dienen. Wie auch bei Arbeitnehmern, die sich zu Verantwortlichen aufschwingen können, wenn sie sich nicht an die Weisungen des Arbeitgebers halten und Daten zu eigenen Zwecken verarbeiten[14], wäre der Betriebsrat gem. Art. 29 DSGVO dann selbst Verantwortlicher, da er sich auf eine Rechtsvorschrift im Sinne des Art. 29 DSGVO nicht mehr berufen kann.

c) Zwischenergebnis

Im Ergebnis lässt sich daher zunächst festhalten, dass vieles dafür spricht, die bisherige Einordnung des Betriebsrates als Teil des Verantwortlichen beizubehalten.

Dieses Ergebnis entspricht auch der datenschutzrechtlichen Verantwortungszuweisung in der Praxis. Denn auch die Schadensersatz- und Bußgeldforderungen bei möglichen Verstößen können sich im Ergebnis nur an rechtsfähige Verantwortliche richten und gerade nicht an Teile der verantwortlichen Stelle selbst.[15] Käme man abweichend zum gegenteiligen Ergebnis, würden sich zahlreiche weitere Umsetzungsfragen stellen. Wäre jedenfalls der Betriebsrat selbst Verantwortlicher im Sinne der DSGVO, wäre er dies grundsätzlich mit allen Rechten und Pflichten.[16] Damit würden ihn bspw. alle Betroffenenrechte selbst treffen. Er müsste bspw. neuen Mitarbeiter gegenüber eigenständig die Informationspflichten gem. Art. 13 bzw. 14 DSGVO erfüllen. Auch wäre ihm gegenüber ein gesondertes Auskunftsrecht geltend zu machen. Es träfe ihn beim Vorliegen der Voraussetzungen auch die Verpflichtung, einen eigenen Datenschutzbeauftragten zu bestellen. Dies wurde bereits unter altem Recht zutreffend als kritisch bewertet.[17] Neben dem Aufwand für betroffene Unternehmen ist hierbei auch die in der Praxis gegebene Möglichkeit unterschiedlicher Ergebnisse und Einschätzungen datenschutzrechtlicher Sachverhalte von nicht unerheblicher Bedeutung.

Die Ergänzung von § 26 Abs. 1 S. 1 BDSG n.F. gegenüber des § 32 Abs. 1 S. 1 BDSG a.F., wonach nunmehr eine Datenverarbeitung zur Ausübung der Rechte und Pflichten einer Interessenvertretung ausdrücklich auch erforderlich sein muss, stellt nach Auffassung des Gesetzgebers lediglich eine Klarstellung dar und ändert insoweit nichts an der vorliegenden Einschätzung.[18]

Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten gem. § 26 Abs. 6 BDSG n.F. bleiben aber auch weiterhin unberührt und sichern die Verantwortung des Betriebsrates für den Beschäftigtendatenschutz.[19]

3. Kontrollrechte des betrieblichen Datenschutzbeauftragten

Besondere Beachtung gilt sodann der Frage, ob dem betrieblichen Datenschutzbeauftragten Kontrollrechte gegenüber dem Betriebsrat zustehen.

Nach einem Urteil des BAG unterliegt der Betriebsrat als Teil der verantwortlichen Stelle zwar den Vorgaben aus dem BDSG a.F.[20], soll aber zugleich vom Kontrollrecht des betrieblichen Datenschutzbeauftragten ausgenommen sein.[21] Für diese Auffassung gibt es keine gesetzliche Verankerung. Das BAG[22] hat allein im Rahmen einer umfassenden Güterabwägung zwischen der besonderen Stellung des Betriebsrates und der Funktion des Datenschutzbeauftragten entschieden, dass die besondere Stellung des Betriebsrates im Unternehmen mit dem Kontrollrecht des betrieblichen Datenschutzbeauftragten unvereinbar sei. Das Spannungsfeld zwischen Betriebsrat und betrieblichem Datenschutzbeauftragten zeigt sich im Gegenzug bei der Auffassung, dass dem Betriebsrat kein Recht und keine Pflicht zur Kontrolle und Überwachung des Datenschutzbeauftragten zukommt.[23] Auch fehlt ihm im Vorfeld bereits ein Mitbestimmungsrecht bei der Bestellung des betrieblichen DSB.[24] Allenfalls steht ihm ein Mitwirkungs- und Mitbestimmungsrecht im Umfeld der Bestellung von internen DSB in seiner Stellung als Arbeitnehmer zu, so es sich beispielsweise um eine Versetzung handelt.[25]

Fraglich ist, ob die im Urteil vorgenommene Güterabwägung noch auf die europäischen Vorgaben aus der Datenschutzgrundverordnung übertragbar ist.

Zunächst beschränkt sich in Ansehung des Wortlautes der DSGVO der

Funktionsumfang des Datenschutzbeauftragten nicht auf bestimmte Einheiten eines Unternehmens. Im Umkehrschluss bedeutet dies: Die Aufgabe gem. Art. 39 Abs. 1 lit. b) DSGVO gilt für die gesamte verantwortliche Einheit ohne Einschränkung. Es gibt keine kontrollfreie Datenverarbeitung – die Datenverarbeitung durch Berufsgeheimnisträger unterliegt ebenso der vollen Kontrolle durch den Datenschutzbeauftragten, wie auch die des Betriebsrates.[26] Insoweit hat der Datenschutzbeauftragte volle Zutritts- und Zugriffsberechtigungen.[27]

Die DSGVO gilt als Verordnung in den Mitgliedstaaten als unmittelbar anzuwendendes Recht, d. h. es bedarf zur Einschränkung des Aufgabenumfanges des betrieblichen Datenschutzbeauftragten einer entsprechenden Öffnungsklausel.

Die Aufgaben des Datenschutzbeauftragten sind in Art. 39 Abs. 1 DSGVO grds. nicht abschließend geregelt, sodass wohl auch die Mitgliedstaaten im Rahmen des Art. 38 Abs. 6 DSGVO dem Datenschutzbeauftragten weitere Aufgaben zuweisen können.[28] Wichtig ist dabei aber, dass es sich um weitere Aufgaben handeln muss. Für eine Beschränkung des Aufgabenumfanges fehlt es hingegen an einer Öffnungsklausel. Überdies ist der Wortlaut gem. Art. 39 Abs. 1 DSGVO insoweit eindeutig, da er festlegt, dass dem Datenschutzbeauftragten „zumindest folgende" in Abs. 1 genannten Aufgaben obliegen.

Eine mögliche Öffnungsklausel, über die durch das BetrVG eine Beschränkung des Aufgabenumfanges des Datenschutzbeauftragten zumindest denkbar wäre, ist Art. 88 DSGVO. Art. 88 DSGVO stellt die Öffnungsklausel für die Verarbeitung im Beschäftigungskontext dar. Danach können die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen. In den Anwendungsbereich der Öffnungsklausel fällt insoweit gerade auch das Betriebsverfassungsgesetz. Den Mitgliedstaaten steht die Befugnis zu nationalen Regelungen aber nicht schrankenlos zur Verfügung, sondern stets nur soweit dies im Rahmen der Vorgaben der Verordnung erfolgt.[29] Jedenfalls wäre die durch das BAG auf Grundlage des BetrVG getroffene Abwägung eine Beschränkung der in der DSGVO normierten Aufgaben des Datenschutzbeauftragten, was jedoch gerade nicht zulässig ist. Art. 88 DSGVO ist mithin keine geeignete Öffnungsklausel, um hierüber Einschränkungen im Aufgabenumfang des Datenschutzbeauftragten zu regeln.[30] Auch über Art. 90 DSGVO kann die Tätigkeit des Datenschutzbeauftragten insoweit nicht beschränkt werden.[31]

Dem Datenschutzbeauftragten steht im Ergebnis ein Kontrollrecht des Betriebsrates zu.

Dabei bleibt zu erwähnen, dass die Ausübung dieses Kontrollrechts nur der Wahrnehmung seiner gesetzlichen Aufgaben zur Kontrolle der datenschutzrechtlichen Vorgaben dient. Dabei unterliegt er keinen Weisungen. Gleichwohl kann es dabei dazu kommen, dass der Datenschutzbeauftragte Kenntnis erlangt über Verarbeitungen personenbezogener Daten, die der besonderen Geheimhaltung nach § 79 Abs. 1 BetrVG unterliegen. § 6 Abs. 5 und Abs. 6 BDSG n.F. bieten hier insoweit nur einen unzureichenden Schutz.[32] Art. 38 Abs. 5 DSGVO normiert allerdings, dass der Datenschutzbeauftragte nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden ist. Entgegen dem Wortlaut handelt es sich dabei aber nicht um einen reinen Verweis in entsprechende Rechtsvorschriften. Vielmehr wird dabei eine umfassende Verschwiegenheitspflicht des Datenschutzbeauftragten auch gegenüber der ihn benennenden Stelle statuiert, die sich auf alle Informationen erstreckt, die zwar einer Kontrolle des Datenschutzbeauftragten, aber keinem Kenntnisrecht der verantwortlichen Stelle unterliegen, wie etwa die Daten des Betriebsrats.[33] Anders als mit solch weitreichender Verschwiegenheitspflicht wäre die Tätigkeit des Datenschutzbeauftragten, welcher im Rahmen seiner Tätigkeit umfassende und auch streng vertrauliche Informationen erhält, die er zur Ausübung seiner Aufgaben auch benötigt, nicht durchführbar.

Umgekehrt hat der Betriebsrat allerdings auch weiterhin kein Kontrollrecht des Datenschutzbeauftragten. Der Betriebsrat unterliegt im Wesentlichen dem nationalen Rechtsgefüge, an dem sich im Verhältnis zum Datenschutzbeauftragten keine Änderung ergibt.[34] Im Verhältnis Betriebsrat zum Datenschutzbeauftragten bleibt es bei den bisherigen Grundsätzen.

4. Resultat

Im Ergebnis lässt sich daher in Übereinstimmung mit der bisherigen Einordnung festhalten, dass der Betriebsrat auch mit Geltungsbeginn der DSGVO in Übereinstimmung mit der bisher herrschenden Meinung Teil der verantwortlichen Stelle bzw. des Verantwortlichen ist, nicht aber selbst Verantwortlicher im Sinne der DSGVO, mithin auch kein Dritter i.S.v. Art. 4 Nr. 10 DSGVO.

Gleichwohl spricht vieles dafür, dass die vom BAG getroffene Abwägung zwischen Stellung und Funktion des Betriebsrates einerseits und der Stellung des betrieblichen Datenschutzbeauftragten andererseits im Rahmen eines gesamteuropäischen Datenschutzkontextes nicht übertragbar ist. Die unmittelbar geltende DSGVO lässt nationale Einschränkungen des Aufgabenbereichs des Datenschutzbeauftragten nicht zu, sodass sich die in der DSGVO normierte Kontrollaufgabe des Datenschutzbeauftragten auch auf den Betriebsrat erstreckt.

Damit hat der Datenschutzbeauftrage nicht nur das Recht, sondern zugleich die Pflicht, den Betriebsrat in seine Kontrollen einzubeziehen.

Im Verhältnis zwischen Betriebsrat und Datenschutzbeauftragtem ist allerdings das sich aus § 2 Abs. 1 BetrVG ergebende Zusammenarbeitsgebot[35] nunmehr von besonderer Bedeutung. Die Zusammenarbeit zwischen Betriebsrat und Datenschutzbeauftragem bekommt unter der Geltung der DSGVO eine neue Gewichtung, denn die ausgeformten und erweiterten Betroffenenrechte der DSGVO sowie die umfassende Etablierung eines Datenschutzmanagements geht nur mit in kooperativer Gemeinschaft.

1 Vgl. Gola/Pötters, RDV 2016, 279 ff.; dem entgegnend Caumanns, RDV 2018, 55f.

2 Vgl. bspw. Gola/Schomerus/Gola/Klug/Körffer, 12. Aufl. 2015, BDSG § 3 Rn. 49; Seifert/Simitis, 8. Auflage 2014, BDSG § 32 Rn. 170

3 Vgl. BAGE 97, 64 = NZA 1998, 385; BAG, AP BetrVG 1972 § 89 Nr. 1 mit Anm. Simitis; BAGE 131, 316 = NZA 2009, 1218; BAGE 140, 350 = NZA 2012, 744 = AP SGB IX § 84 Nr. 4 mit Anm. Kort; BAG, NZA 2013, 49; BAG, NZA 2014, 738; So zuletzt auch das LAG München bei zum möglichen Anspruch des Betriebsrats auf namentliche Benennung von schwangeren Mitarbeiterinnen auch gegen deren Willen, LAG München, Urteil vom 30.11.2017 - 3 O 182/17 = ZD 2018, 226 ff.

4 WP 169, „Für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 16

5 Vgl. auch Gola/Pötters, RDV 2016, 279 (279)

6 Ehmann/Selmayr/Klabunde, 1. Aufl. 2017, EU-DSGVO Art. 4 Rn. 25

7 Caumanns, RDV 2018, 55

8 Caumanns, RDV 2018, 55

9 Caumanns, a.a.O.

10 Vgl. hierzu Pötters/Gola, RDV 2017, 279 ff, andere Auffassung Caumanns, a.a.O.

11 Kühling/Buchner/Hartung, 2. Auflage 2018, DSGVO Art. 4 Nr. 7 Rn. 9 ff.

12 Pötters/Gola, RDV 2017, 279 (280)

13 Pötters/Gola, RDV 2017, 279 (281)

14 Kühling/Buchner/Hartung, 2. Auflage 2018, DSGVO Art. 4 Nr. 7 Rn. 10

15 Pötters/Gola, RDV 2017, 279 (280, 281)

16 So auch Caumanns, RDV 2018, 55 (56)

17 Kort, NZA 2015, 1345 (1349)

18 Pötters/Gola, RDV 2017, 279 (281)

19 Vgl. Pötters/Gola, RDV 2017, 279 (282)

20 BAGE 131, 316 = NZA 2009, 1218 (1220, 1221)

21 Vgl. BAGE 97, 64 = NZA 1998, 385 (386, 387)

22 Siehe Fn. 21

23 Kort, NZA 2015, 1345 (1349) m.w.N.

24 NZA 2015, 1345 (1351)

25 Kort, NZA 2015, 1345 (1349 f.); BAGE 97, 64 = NZA 1998, 385 (387)

26 Kühling/Buchner/Bergt, 2. Aufl. 2018, DSGVO Art. 38 Rn. 18

27 Kühling/Buchner/Bergt, 2. Aufl. 2018, DSGVO Art. 38 Rn. 19

28 Kühling/Buchner/Bergt,2. Aufl. 2018, DSGVO, Art. 39 Rn. 24

29 Selk/Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 88 Rn. 51

30 Vgl. auch Kühling/Buchner/Bergt, 2. Aufl. 2018, DSGVO Art. 38 Rn. 18

31 Kühling/Buchner/Bergt, 2. Aufl. 2018, DSGVO Art. 38 Rn. 18

32 Vgl. Pötters/Gola, RDV 2017, 279 (283)

33 Kühling/Buchner/Bergt, 2. Aufl. 2018, DSGVO Art. 38 Rn. 38-38a

34 Zur Begründung vgl. Kort, NZA 2015, 1345 (1351);

35 Kort, NZA 2015, 1345 (1351)

Heinz Alenfelder

40 Jahre DANA – Rückblick eines nicht völlig Unbeteiligten

Als ich nach vielen Jahren erneut in den DVD-Vorstand gewählt wurde, kam dort die Idee auf, ich könne einen Rückblick zum DANA-Jubiläum verfassen. Eine Nabelschau sollte dies nicht werden, aber für mich, der ich die Datenschutz-Nachrichten über nahezu die gesamten 40 Jahre hinweg bezogen und teilweise aktiv begleitet habe, war das Jubiläum Anlass, weit über einhundert Ausgaben der Zeitschrift zu durchforsten und stundenlang in alten Artikeln zu schmökern. Dabei erwies sich die DANA als ein Medium, das die Entwicklung des Datenschutzes in Deutschland nachzeichnet und zugleich verdeutlicht, wie sich die Informationsvermittlung und Interessenvertretung unserer Bürgerrechts-Organisation im Laufe der Jahrzehnte verändert hat.

Im Jahr nach der Gründung der DVD erschien die erste DANA-Ausgabe 1-1978. Prof. Peter Gola, DVD-Gründungsmitglied, positionierte die DANA als wichtige deutsche Fachzeitschrift für Datenschutz. Er ließ sie als Zeitung (ISSN 0173-7767) registrieren und räumte von Beginn an die Möglichkeit eines Abonnements ein. So entwickelte sich neben den DVD-Mitgliedern ein fester Kundenstamm aus Wissenschaft und Praxis. Zunächst einspaltig mit Schreibmaschine getippt, später dann zweispaltig etwas leichter lesbar, war die DANA ein nüchternes Fach-Magazin, die Seiten frei von jeglichem Bildmaterial. Erst nach 10 Jahren wurden die zweispaltigen Schreibmaschinenseiten dann per Computer erstellt (wenn auch anschließend noch mit Schere und Kleber sowie wenig originellen Karikaturen aus einem copyright-freien Schnibbelbuch fertig gestaltet).

Mit den auf Gola folgenden DVD-Vorstandsmitgliedern, die die gestalterische Verantwortung für die DANA hatten (1987-1996 der Autor dieser Zeilen, 1997-2009 Hajo Köppen mit Unterbrechung, 2005-2007 Rainer Scholl und seit 2010 Frans Valenta), nahm die Fortentwicklung der äußeren Erscheinung ihren Lauf. Nicht nur die Umschlagseiten wurden modernisiert, mit jedem Wechsel erhielt die DANA sozusagen ein neues Gesicht. Waren bis 1987 statt der geplanten sechs Ausgaben pro Jahr auch mehrmals lediglich drei Doppelhefte erschienen, legte sich Hajo Köppen 1997 auf vier Ausgaben pro Jahr fest – jeweils zum Quartals-Ende. Bei steigender Qualität und wachsendem Umfang zeichnet sich die



Preisentwicklung der DANA durch Stabilität aus: Die erste Erhöhung erfolgte nach 17 Jahren, die zweite mit der Euro-Umstellung auf 32 Euro und seit 2014 beträgt der Abonnement-Preis 42 Euro inkl. Porto.

Unter der Redaktion von Peter Gola lag der Schwerpunkt der frühen DANA-Jahre auf der Veröffentlichung juristisch einschlägiger Fachbeiträge. Dies änderte sich mit dem ersten Wechsel in der Redaktion. Der DVD-Vorstand kommentierte in Heft 1/2-1985:

„Umfang und Gestaltung der ‚Datenschutz-Nachrichten' haben sich ebenso gewandelt wie die inhaltlichen Lese-Angebote. Verstärkt wurde auf eine Informationsvermittlung über Datenschutz für den Datenschutzbetroffenen Wert gelegt, die Datenschutz verständlich und begreifbar machen sollte".

Die Informationsvermittlung wurde ergänzt um konkrete Anregungen in Form von Postkarten, Musterbriefen und auch Adresslisten. Ab 1993 kam zu allgemeinen Datenschutz-Nachrichten auch speziell eine Rubrik über Zeitungsberichte hinzu, die Jahre später um Nachrichten aus dem WWW erweitert wurde. Die ersten 10 Jahre der Big Brother Award-Verleihungen in Bielefeld wurden intensiv dokumentiert, bis diese einer solchen publizistischen Unterstützung nicht mehr bedurften. Kurzum: In Schwerpunktheften wurde von Gesetzesentwürfen und Verordnungen über Stellungnahmen bis zu entsprechenden Presseerklärungen breit gefächert so ziemlich alles rund um den Datenschutz veröffentlicht, was sich heute mehr oder weniger schnell im WWW finden lässt. Auch PDF-Versionen der DANA sind mittlerweile unter www.datenschutzverein.de online abrufbar.

Viele Autorinnen und Autoren aus befreundeten Organisationen, Wissenschaft und Praxis lieferten Beiträge zu Schwerpunktheften, doch eine große Zahl von Artikeln und alle kleinen Nachrichten stammem aus der Feder von DVD-Vorstandsmitgliedern, die früher wie heute reihum die inhaltliche Verantwortung für einzelne Hefte übernehmen. Von der Rolle der DANA als „Vereinsorgan" zeugen regelmäßige Aufrufe zur Mitarbeit, mehrere Postkarten-Aktionen und auch Beiträge in Schwerpunktheften. Das wird beispielhaft deutlich am folgenden Zitat aus dem Heft 5/6-1990, Schwerpunkt „DVD-intern":

„Die Arbeit der Deutschen Vereinigung für Datenschutz war im Jahre 1990 und ist in den ersten Wochen dieses Jahres (1991) von einem politischen Umfeld geprägt, in dem Datenschutz an und für sich zu einem Randthema werden muss(te). ... (erwähnt werden Golfkonflikt und Zusammenschluss der beiden deutschen Staaten) ... Datensammler tragen zum Abbau der demokratischen Freiheitsrechte in unserer Gesellschaft bei. Der Widerstand soll eingeschränkt werden. Die Masse wird verplant. Die Aufgabe der DVD besteht nun darin, auf die Gefahren des Einsatzes von Informationstechnologien aufmerksam zu machen, sie abzuwehren."

Ebenso deutlich positioniert das Editorial des Heftes 1/2-1991 den Verein und auch seine Zeitschrift. Das damals neue BDSG („Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes") wurde abgedruckt und eingeschätzt:

„... strotzt von Gedanken und Vokabeln der 1960er und 1970er Jahre. ... Alles läuft darauf hinaus, daß die Betroffenen sich engagieren müssen, um ihre Rechte durchzusetzen. Hilfestellung will dabei die Deutsche Vereinigung für Datenschutz bieten. Lautete ihre Hauptparole in den Anfangsjahren ‚Wache Bürger – Sichere Daten', so hat sich diese Sicht mittlerweile grundlegend geändert. Weder gibt sich der Verein der Illusion hin, Wachheit allein könne etwas bewirken, noch steht die Datensicherheit im Mittelpunkt. Heute, nach 15 Jahren harter Arbeit, wird das Motto am besten mit ‚Gemeinsam für die Verwirklichung von Freiheitsrechten' umschrieben."

In diesem Sinne wird wohl – ohne dass sie heute noch abgedruckt werden müsste – für das kommende Jahrzehnt die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) als Basis der Arbeit der DVD und der Inhalte der DANA dienen.

Das Motto bleibt unverändert: Die Verwirklichung von Freiheitsrechten.

Klaus-Jürgen Roth

BigBrotherAwards 2018 [Bilder: digitalcourage]

Mit BigBrotherAwards (BBA) zeichnet der Verein Digitalcourage e. V. gemeinsam mit weiteren Organisationen (Internationale Liga für Menschenrechte e. V. – ILFM, Deutsche Vereinigung für Datenschutz e. V. – DVD, Netzwerk Datenschutzexpertise, Chaos Computer Club e. V – CCC) jedes Jahr Datensünder aus. Die Preisträger haben nach Ansicht der JurorInnen besonders massiv gegen Datenschutz-Grundsätze verstoßen. Die BigBrotherAwards werden seit dem Jahr 2000 verliehen.

Im Jahr 2018 gingen die in sechs Kategorien verliehenen Preise an folgende Preisträger:

- **Soma Analytics** für die Gesundheits-App Kelaa und das damit verbundene Kelaa Dashboard (Kategorie Gesundheit),
- das Konzept der **Smart City** (Kategorie PR und Marketing),
- **Microsoft Deutschland** (Kategorie Technik) für das Betriebssystem Windows 10,
- **Cevisio Software und Systeme** für die in Flüchtlingsunterkünften eingesetzte Software Cevisio Quartiersmanagement (Kategorie Verwaltung),
- **Amazon**, für dessen „smarten“ Sprachassistenten Alexa (Kategorie Verbraucherschutz),
- die **Fraktionen von CDU und Grünen im hessischen Landtag** für das geplante neue Verfassungsschutzgesetz (Kategorie Politik).

Firmen verkaufen das, was sie an Daten über Menschen eingesammelt haben, als aggregierte korrekte Darstellung der Realität, was tatsächlich aber eine Big-Data-Illusion ist. Dies erklärte Sarah Spiekermann zum Auftakt der Verleihung der BigBrotherAwards. Mit großem Elan wird der eingesammelte Secondhand-Eindruck zum digitalen Abdruck erklärt, gar zum Öl des 21. Jahrhunderts verklärt, weil die künstliche Intelligenz mit diesen Daten gefüttert wird und Algorithmen die Secondhand-Sammlung aufbereiten. Für Spiekermann ist es höchste Zeit, dass diese Blase platzt.

In den Laudationes wurden die genauen Gründe der Auswahl der diesjährigen Awards dargelegt.

Soma Analytics

In Aldous Huxleys Zukunftsroman „Schöne neue Welt“ ist „Soma“ eine stimmungsaufhellende Droge, die vor dem Sex eingenommen oder auch als Dampf verteilt wird, um negative Stimmungen und kritisches Denken in der Bevölkerung auszuschalten. Insofern gibt das deutsche Healthtech-Startup Soma Analytics aus der Nähe von München schon im Namen zu erkennen, dass es sich mit Stimmungsaufhellern beschäftigt und dafür auch EU-Forschungsmittel erhalten hat. Herausgekommen ist eine Smartphone-App namens Keela Mental Resilence, die Stressdaten der Beschäftigten an ein Keela Dashboard überträgt, das fortlaufend über den „Gemütszustand“ eines Teams, das „Wohlbefinden“ einer Abteilung oder gleich über das „Stresslevel“ einer ganzen Firma informiert.



Peter Wedde

Für den Juror, den Arbeitsrechtler Peter Wedde von der Frankfurter Akademie der Arbeit begeht Soma Analytics mit der Übergabe von Gesundheitsdaten in die Hände von Arbeitgebern einen Tabubruch, auch wenn die Daten, wie Soma Analytics betont, nur in aggregierter und anonymisierter Form vorliegen. Besonders bedenklich sei die Empfehlung der Stresserkenner, das Smartphone abends mit ins Bett zu nehmen, damit die Sensoren Daten über das Schlaf- und Beischlafverhalten sammeln können. In den rechtlichen Hinweisen der Firma fehle eine zumindest in Deutschland notwendige Zustimmung der Beschäftigten nach dem noch geltenden Bundesdatenschutzgesetz wie nach der kommenden DSGVO. Die App Keela, mit der zahlreiche Daten zum Wohlbefinden oder zum Unwohlsein eingesammelt werden, reihe sich ein in die Klasse der Softwareangebote für Predictive Analytics, bei der Vorhersagen getroffen werden, die so konkret sein können, dass der Einzelne trotz Anonymisierung identifiziert werden kann. Grundsätzlich sei nichts dagegen einzuwenden, wenn jemand eine App einsetzt, um Stress zu vermeiden oder zu verringern. Nur sollte die App nicht dem Arbeitgeber gehören.

Die Firma Soma Analytics beschwerte sich als Preisträgerin in der Person des Geschäftsführers Johann Huber über den Prozess, der zur Verleihung des Preises führte: „Wir wurden vor der Nominierung nicht kontaktiert, um die Richtigkeit der Gründe der Nominierung zu prüfen, auch wurden uns andere Gründe genannt als den Medienpartnern“. Er wirft den Machern des BigBrotherAwards vor, unter anderem auf Basis von längst veralteten Informationen entschieden zu haben. Die Begründung für die Vergabe des Award, nämlich dass die App „anhand verschiedener Parameter (z. B. Aufgeregtheit der Stimme beim Telefonieren) den Gesundheits- und Vitalzustand des Nutzers“ überwache, waren auch nach der Preisvergabe auf der Webseite von Soma Analytics abrufbar. Huber erwiderte: „Ein Blick in unsere öffentlich zugängliche Datenschutzerklärung hätte gezeigt, dass die Kelaa Smartphone-App keinen Zugang auf

die Stimme beim Telefonieren zulässt." In den englischsprachigen aktuellen Nutzungsbedingungen ist von dieser Anwendung keine Rede. Huber kündigte auf journalistische Anfragen hin an, veraltete Information von 2013, wonach auch Telefonie-Daten ausgewertet würden, zu aktualisieren. Man habe in der Vergangenheit tatsächlich mit einem Tracking-Feature für Sprachanrufe experimentiert. Dies sei aber wieder verworfen worden, „eben genau wegen Privacy-Bedenken". Auch die noch online zu findende Idee einer Stimmanalyse per Sprachaufzeichnung sei wieder verworfen worden und nie über „interne Tests" hinausgegangen.

Smart Cities

Richtige Smart Cities, in denen die Straßenlampen die BürgerInnen beleuchten, ihnen bei Bedarf Strom spenden und diese fürsorglich überwachen, sind noch ein Stück weit Zukunftsmusik. Doch das Konzept ist da und verdiente nach Ansicht der BBA-Jury einen Preis, vergeben in der Kategorie PR und Marketing. In Ländern wie China, Türkei und Aserbaidschan feilt man energisch an der Überwachungskomponente, während bei uns die Bewirtschaftung des Parkraums im Vordergrund steht. Doch die intelligente Stadt hat Zukunft, weil der Trend zur Mega-Agglomeration anhält. Da können smarte Sachen helfen, wenn sie die BürgerInnen nicht nur um die Staus herumlotsen, sondern auch um Schießereien hier und da. Wo die Smart City aufhört, fängt der Polizeistaat an, etwa wenn die Gesichtserkennung in smarten Lampen die BürgerInnen unter Generalverdacht stellt. John Sudworth, ein Reporter der BBC, ließ



Rena Tangens bei der Laudatio zu Smart Cities

sich in einer chinesischen Stadt suchen und war nach wenigen Minuten fürsorglich umlagert.

Gerade weil die neue Bundesregierung in ihrem Koalitionsvertrag davon spricht, das Konzept der „intelligenten Videoüberwachung" auszubauen, hat Smart City nach Ansicht der JurorInnen einen Preis verdient, ohne dass eine einzelne Firma oder eine Stadt ausgezeichnet wird. Die Laudatorin Rena Tangens: „Eine Smart City ist die perfekte Verbindung des totalitären Überwachungsstaates aus George Orwells 1984 und den normierten, nur scheinbar freien Konsumenten in Aldous Huxleys Schöne Neue Welt".

Microsoft



Frank Rosengart bei der Laudatio zu Microsoft

Eine der ersten Firmen, die nach Bielefeld kamen, war Microsoft im Jahre 2002, als Microsoft in der etwas seltsamen Kategorie „Lebenswerk" einen BigBrotherAward für ihr Digital Rights Management (DRM) namens Palladium bekam. Damals schickte Microsoft den Datenschutzbeauftragten Sascha Hanke, der das DRM-System verteidigte. 16 Jahre später erhielt das Unternehmen nun den Preis in der Kategorie Technik für sein Betriebssystem Windows 10. Dort gibt es eine ganze Reihe von Funktionen, die Daten an Microsoft übermitteln. Dementsprechend muss an einer ganzen Reihe von Schräubchen gedreht werden, wenn man die Datensammelei beherrschen will. Microsoft bestätigt dies in seinem Privacy Statement, wendet sich aber zugleich gegen die Forderung von Datenschutzbeauftragten, die Datenübertragung bei Windows 10 abzuschalten. Gegen die Datenübermittlung gewendet, fordert die BBA-Jury von Microsoft mindestens eine Option „übermittele gar nichts" neben den Auswahlpunkten einer „einfachen" und einer „vollständigen" Datenübermittlung. Spätestens mit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) müsse Microsoft dafür Sorge tragen, dass „keine Übermittlung" eine Option ist, die standardmäßig aktiviert sein sollte. Ansonsten würden Microsoft-Produkte zu einem nicht mehr tragbaren Problem, so Frank Rosengart vom Chaos Computer Club in seiner Laudatio. Microsoft betonte in Reaktion auf die Preisverleihung, Datenschutz sei ein wichtiges Ziel des Unternehmens; man gebe für Verbesserungen in diesem Bereich pro Jahr rund eine Milliarde Dollar aus.

Fraktionen von CDU und Bündnis 90/ Die Grünen im hessischen Landtag

Die hessischen PolitikerInnen bekommen den Preis, weil der schwarz-grüne Gesetzentwurf zum Verfassungsschutzgesetz, so Rolf Gössner von der ILFM, „eine gefährliche Anhäufung schwerwiegender Überwachungsbefugnisse" für den Staat vorsehe. Die konkreten Mittel seien ein „schwerer Angriff auf Demokratie, Rechtsstaat und Bürgerrechte". Eigentlich sind die Grünen mit Experten wie Jan-Philipp Albrecht oder Konstantin von Notz eine Partei, die Bürgerrechte und den Datenschutz ernst nimmt. In Hessen, wo Joschka Fischer in Turnschuhen das erste Mitregierungsprojekt einleitete, richtet sich zumindest die Landtagsfraktion anderweitig aus. Sie erhielten für das „Gesetz zur Neuausrichtung des Verfassungsschutzes" gemeinsam mit der CDU-Faktion den BigBrotherAward in der Kategorie Politik. Beide Parteien wollen, dass nicht nur die Polizei in der Strafverfolgung, sondern auch der Verfassungsschutz als Nachrichtendienst Hessentrojaner einsetzen darf, um verdächtige Gefährder mit Hilfe der Quellen-TKÜ und der heimlichen Online-Durchsuchung zu überwachen. Zusätzlich sollen erkannte Gefährder zum Tragen einer elektronischen Fußfessel verurteilt werden können, um künftige Straftaten zu entdecken. Der Verfassungsschutz soll künftig auch vorbestrafte V-Leute einsetzen und V-Leute im beruflichen Umfeld von Ärzten, An-

wälten und Journalisten platzieren dürfen. Eine weitere Spezialität schwarzgrüner Überwachung ist die Erlaubnis, dass der Verfassungsschutz Daten von Kindern unter 14 Jahren speichern darf. Dazu passt dann der Einsatz des Nachrichtendienstes als Auskunftei, wenn die Überprüfung der Verfassungstreue bei Einstellung im öffentlichen Dienst ansteht.



Rolf Gössner

Als Laudator des Politikpreises kam stilgerecht der Rechtsanwalt Rolf Gössner zum Einsatz. Gössner wurde seit den 70er Jahren bis in die jüngste Zeit vom Verfassungsschutz überwacht. Während dieser Zeit wurde er u. a. als Referent zu einer Tagung des hessischen Verfassungsschutzes eingeladen, zum direkten Erfahrungsaustausch zwischen Schnüfflern und Ausgeschnüffelten. Für Gössner ist es ein Unding, wenn die Grünen im hessischen Landtag behaupten, diese „Neuausrichtung des Verfassungsschutzes" würde eine „grüne Handschrift" tragen. Was nach den Pannen und Skandalen bei der Aufdeckung der NSU-Mordserie zu einer Neuausrichtung führen sollte, sei zu einer umfassenden Blankovollmacht für den Ausbau des Geheimdienstes mutiert: „Doch stattdessen erhalten ausgerechnet diese demokratisch kaum kontrollierbaren Geheimbehörden des Bundes und der Länder – geschichtsvergessen muss man sagen – wieder unverdienten Auftrieb, werden abermals aufgerüstet und massenüberwachungstauglicher gemacht, anstatt die Bevölkerung endlich vor ihren klandestinen Machenschaften und Skandalen wirksam zu schützen,"

Jürgen Frömmrich, innenpolitischer Sprecher der Grünen-Landtagsfraktion in Hessen, zeigte sich überrascht vom Preis. Man habe von der Verleihung konkret an die Fraktion erst durch Anfragen von Journalisten erfahren. Frömmrich wurde als Befürworter des Verfassungsschutzgesetzes von seiner Partei bei der Aufstellung der Landesliste für die nächste Landtagswahl auf einem kurz nach der BBA-Verleihung durchgeführten Parteitag abgestraft und landete auf dem Landeslistenplatz zwölf – nicht wie angestrebt auf Platz acht. Auf Platz acht wurde der Software-Experte Torsten Leveringhaus gewählt, der sich „gegen die digitale Aufrüstung" ausgesprochen hatte. Der Publikumspreis der BigBrotherAwards 2018 ging mit großem Abstand an die Fraktionen von CDU und Bündnis 90/Die Grünen im Hessischen Landtag.

Cevisio

Schutzlose Flüchtlinge und Asylbewerber werden mit Hilfe einer Software für das „Quartiersmanagement" von Cevisio-Software verwaltet. Sie werden dort wie Sachen behandelt und mit Hilfe von Chipkarten-Systemen dauerüberwacht, bis hin zur Essensausgabe oder der Teilnahme an angebotenen Aktivitäten. Begründet wird dies damit, dass man bei Ausbruch eines Feuers wissen müsse, wer sich aktuell in der Unterkunft aufhält. Träfe die Begründung zu, müsste jede Schule solche Systeme besitzen, so die BBA-Jury. Deshalb bekommt die Software, die Cevisio aus Torgau/Sachsen mit Unterstützung des dortigen Roten Kreuzes entwickelt hat, einen Preis in der Kategorie Verwaltung, stellvertretend für eine ganze Reihe von Systemen, die Daten über Flüchtlinge in ausufernder Weise speichern. Die Chipkarte kontrolliert Bewegungen auf dem Gelände, trackt die Essenausgabe und stellt medizinische Checks wie durchgeführte Röntgen-, Blut- und Stuhluntersuchungen bis hin zu Verwandtschaftsverhältnissen, Religions- und Volkszugehörigkeiten zur Verfügung. All dies wird von der Software abgefragt und mit anderen Dateien nach dem „Datenaustauschverbesserungsgesetz" verknüpft, insbesondere mit dem 2016 eingeführten Kerndatensystem für Asylsuchende.

Besonders problematisch ist für Laudator Thilo Weichert von der DVD und dem Netzwerk Datenschutzexpertise, dass Cevisio als Softwarehersteller in seinen Unterlagen keinerlei Angaben zum Schutz der Daten von 380.000 Flüchtlingen mache, die aktuell von der Software verwaltet werden. Die Firma wirbt mit dem Slogan „Software, die glücklich macht". (siehe die gesamte Laudatio S. 97)

Amazon



Padeluun

Bei Amazons Alexa monierte der Laudator Padeluun, dass die Sprachaufnahmen in der Cloud verarbeitet werden und auch Monate später noch abrufbar sind. Das „geschwätzige Lauschangriffdöschen" überwache alle Haushaltsmitglieder. Was heute von ahnungslosen VerbraucherInnen praktiziert wird, die sich einen mithörenden Assistenten in die Wohnung stellen, bringt Padeluun von Digitalcourage auf die Palme. Für ihn ist Amazons Alexa – stellvertretend für Siri, Google Assistant, Microsofts Cortana, Samsung Bixby und Nuance ausgezeichnet – „eine Abhörschnittstelle, die sich zum Beispiel als Wecker tarnt, aber ein allwissender Butler in fremden Diensten ist, der sich von mir höchstpersönlich ins Schlafzimmer tragen und an das weltweite Überwachungsnetz anschließen lässt." Alexa steht in der Tradition von „Hello Barbie", die im Jahr 2015 gekonnt einen Preis abräumte, und macht Amazon zum Seriensieger. Amazon Logistik und der Mechanical Turk von Amazon konnten ebenfalls 2015 punkten.

Es ist keine Frage, dass mit Alexa, Siri, Cortana und Co. die Verarbeitung natürlicher Sprache der nächste große Sprung in der Entwicklung der universalen „Benutzeroberfläche" ist. Selbst ein alter Digitalhase wie Padeluun schwärmt davon,

wenn er beim Nudelkochen mit „Alexa, Timer 8 Minuten" den Kurzzeitwecker einstellen kann. Doch der Verbund mit der dahinter liegenden Kontrollstruktur sei problematisch, unter vielen Aspekten. So berichtete unlängst die Süddeutsche Zeitung, dass die Polizei im US-Bundesstaat Arkansas in einem Mordfall Alexa in den Zeugenstand berufen wollte, weil der Mord vom System möglicherweise aufgezeichnet wurde. Der Widerstand gegen Alexa ist für die MacherInnen hinter dem BigBrotherAward gleichbedeutend mit dem Widerstand gegen den großen Lauschangriff und alle Überwachungsmaßnahmen, die mit der Verabschiedung der Notstandsgesetze vor 50 Jahren begann, als die G10-Gesetze zur Telefonüberwachung eingeführt wurden.

Amazon verteidigte seinen Lautsprecher: „Alle Daten sind während der Übertragung und in der Cloud verschlüsselt. Der Kunde behält jederzeit die volle Kontrolle über seine Sprachaufzeichnungen. Jede einzelne Aufnahme kann einfach über die Alexa App oder Amazon.de gelöscht werden" (Gruber, Negativpreis geht an Amazon und Microsoft, www.spiegel.de 20.04.2018; Borchers, Die Big Brother Awards 2018: Von Windows 10, eHealth, Hessentrojanern und anderen Datenkraken, www.heise.de 20.04.2018; Faber, Was war. Was wird. Mit einer Nachlese zu den Big Brother Awards, www.heise.de 22.04.2018; umfassend: bigbrotherawards.de/; Digitalcourage Newsletter 26.04.2018).



Thilo Weichert

Thilo Weichert

Der BigBrotherAward 2018 in der Kategorie Verwaltung geht an die

Cevisio Software und Systeme GmbH aus Torgau

für ihre Software „Cevisio QMM" (Quartiersmanagement), die in Zusammenarbeit mit dem Deutschen Roten Kreuz speziell für Flüchtlingsunterkünfte entwickelt wurde. Mit dieser Software werden Bewegungen zum und auf dem Gelände, Essenausgaben, medizinische Checks wie durchgeführte Röntgen-, Blut- und Stuhluntersuchungen, Verwandtschaftsverhältnisse, Religions- und Volkszugehörigkeiten und vieles mehr erfasst und gespeichert. Die Daten ermöglichen eine Totalkontrolle der Flüchtlinge und zeigen anschaulich, auf wie vielen Ebenen Privatsphäre verletzt werden kann.

Die Software ist nicht nur preiswürdig wegen der mit ihr möglichen Datenschutzverstöße, sondern vor allem wegen des Menschenbildes, das dahinter steht. Flüchtlinge sind Menschen, keine Sachen. Sie liegen nicht in einem Regal zur späteren Abholung und Verwendung, sie sind keine Gefangenen und bedürfen keiner verschärften Beobachtung. Sie suchen Schutz bei uns und haben Rechte – Menschenrechte und Grundrechte, die für Cevisio keine Rede wert sind.

Als 2015 viele Flüchtlinge nach Deutschland kamen, war das Chaos bei Behörden groß. Die Erhebung von Daten sowie die Organisation von Unterbringung und Versorgung stellten die Beteiligten vor große Herausforderungen. Der Mittelständler Cevisio erarbeitete mit dem Deutschen Roten Kreuz Landesverband Sachsen e.V. die Lösung. Das Unternehmen wirbt für seine Software auf seiner Homepage damit, dass sie in über 280 Aufnahmeeinrichtungen eingesetzt wird. Insgesamt würden „bereits mehr als 380.000 Flüchtlinge verwaltet."

Über all diese Menschen liegen demnach in der Cevisio Quartiersmanagement-Software erfasste Daten vor. Basis für die Erfassung ist eine Ausweiskarte mit RFID-Chip oder Barcode. Mit dieser Karte bewegen sich die BewohnerInnen in ihrer Unterkunft und – so der Plan der Software-Macher – halten sie an verschiedenen Stellen vor ein Lesegerät: Am Ein- und Ausgang, bei der Essensausgabe, bei der Wäschestelle, wenn sie Taschengeld bekommen, beim Ausleihen von Büchern oder Videofilmen, bei medizinischen Untersuchungen oder bei ehrenamtlicher Arbeit.

Diese in den Unterkünften erfassten sogenannten „Aktionen" führt die Software über Schnittstellen zusammen mit den Daten des Bundesamtes für Migration und Flüchtlinge – dem BAMF – und mit den Dateien der Ausländerbehörden. Erfasst werden u. a. Angaben zu bestehender Schwangerschaft, zu den verwandten Personen, medizinische Daten mit „Erst- und Folgeuntersuchungen inkl. Befund". Gewährleistet wird auch die Erfassung „sämtlicher Dokumente". Die Software ermöglicht damit nicht nur die „Verwaltung", sondern auch die (Zitat) „Abrechnung der Flüchtlinge". Sie erlaubt die „Erfassung sämtlicher Daten zum Asylverfahren, wie EASY-Optimierung und BAMF-Daten".

Das ist Totalkontrolle. Tagesabläufe, Gewohnheiten, Kontakte, Verwandtschaft, Gesundheitszustand, Asylstatus – alles an einem Ort. Verknüpft und auswertbar.

Manches ist sicher sinnvoll, z. B. Hinweise auf Allergien, oder ob spezielle Ramadan-Verpflegung gewünscht wird. Die Cevisio-Software geht aber deutlich weiter: In der Broschüre zum Funktionsumfang ist z. B. die Rede von der „Erfassung aller an eine Person ausgegebenen Mahlzeiten" sowie „Hinweis bei Mehrfachausgabe einer Mahlzeit an eine Person". Wofür braucht man das?

Ist es nötig, jede Bewegung ins Haus oder aus dem Haus heraus minutiös zu erfassen und zu speichern? Ja, sagt die besagte Broschüre (Zitat): „Über die integrierte Anwesenheitsübersicht ist immer sekundenaktuell erkennbar, welche Flüchtlinge und Helfer/Mitarbeiter sich aktuell in einer Unterkunft befinden. Neben einer reinen Kontrollfunktion ist diese Übersicht insbesondere im Katastrophenfall (Brand etc.) unverzichtbar."

„Unverzichtbar!" Es kommt einem fast seltsam vor, dass hunderttausende von Schulen, Kaufhäusern oder Jugendherbergen noch ohne eine solche sekundenaktuelle Übersicht auskommen. Sind die alle verantwortungslos?

Nein, das ist Leben. Inklusive einem gewissen Lebensrisiko. Die Datensammlung von Cevisio hingegen ist ein feuchter Traum für Überwachungs-Fanatiker. Wir sehen hier keinerlei Empathie mit Menschen, die auch wegen eines Lebens in Freiheit nach Deutschland geflüchtet sind.

Vielleicht ist es also Pragmatismus nach dem Motto „interessiert doch keinen", wenn das Wort „Datenschutz" in der 15-seitigen Systemdarstellung nicht ein einziges Mal vorkommt. Technische Datensicherheitsvorkehrungen verbergen sich hinter dem Begriff „Administration". Funktionalitäten zu den Betroffenenrechten, z. B. für eine Auskunftserteilung oder Transparenz für die Flüchtlinge, konnte ich nicht finden.

Auch in der Praxis gibt es Mängel: Die Datenschutzbeauftragte in Bremen äußert in ihrem aktuellen Jahresbericht „erhebliche datenschutzrechtliche Bedenken". Speicherfristen waren viel zu lang. Weshalb jede Essensausgabe kontrolliert werden muss, erschloss sich ihr nicht. Die Speicherung der Gesundheitsdaten musste auf ihre Veranlassung massiv zurückgefahren werden. Bei Verwandtschaftsangaben wurde den Betroffenen keine Optionen eröffnet. Viele Fragen sind bis heute offen.

Die bremische Datenschutzkontrolle bezog sich nur auf wenige der Einrichtungen. Es besteht keine Gewähr und Kontrollmöglichkeit, dass in den anderen über 270 Einrichtungen rechtswidrige Überwachungsmöglichkeiten abgestellt werden. Die Rechtslage ist überall gleich und könnte, z. B. mit automatischen Löschfristen, in der Software voreingestellt sein. Cevisio könnte den Betreibern Hilfen und Hinweise zur Wahrung des Datenschutzes geben.

Wir fragen: Hat diese Softwaregestaltung damit zu tun, dass hier Flüchtlinge die Betroffenen sind? Sicher – Flüchtlingsunterkünfte sind logistisch komplexe Systeme und die Betreiber wie das DRK und andere können digitale Unterstützung gut gebrauchen. Doch wie sollen Flüchtlinge sich bei uns integrieren, wenn ihnen dabei die Werte unserer gern beschworenen Leitkultur vorenthalten werden, also die Werte unseres Grundgesetzes? Zu diesen Werten gehört Selbstbestimmung, das Recht auf informationelle Selbstbestimmung.

Die Cevisio Software „Quartiersmanagement" steht nur exemplarisch für einen bevormundenden, intransparenten und überwachungsgierigen Umgang mit Flüchtlingen generell. Da gibt es Schweigepflichtentbindungen der Bundesagentur für Arbeit, die alle und jeden von der Vertraulichkeit entbinden, einschließlich Sozialämter und Migrationsberatungsstellen. In einem sog. Datenaustauschverbesserungsgesetz wurde 2016 festgelegt, dass praktisch jede Stelle jede andere über Flüchtlinge unterrichten darf, wenn es erforderlich erscheint. Um die Herkunft von Flüchtlingen bestimmen zu können, ließ sich das BAMF den Zugriff auf die Smartphones der Flüchtlinge genehmigen, auf denen sämtliche Kommunikationen und viel Privates gespeichert sind.

Gleichzeitig berichten unabhängige Flüchtlingsberatungen, dass ihnen manche Behörden mit dem Verweis auf den Datenschutz Informationen verweigern, die für Beratung und Hilfestellung wichtig wären. Hier wird der Datenschutz als falscher Vorwand missbraucht, um soziale Arbeit zu behindern.

Beim Umgang mit den Daten von Flüchtlingen müssen wir besonders umsichtig sein. Sowohl die Nationalsozialisten als auch das DDR-Regime haben mit Informationen und Datenerfassung ihre Bevölkerung kontrolliert und malträtiert. Die Regierungen der Länder, aus denen Menschen zu uns flüchten, quälen ihre Bevölkerung nicht selten durch Kontrolle, Willkür und Verwendung von dem, was sie über diese Menschen wissen. Die Gefahren, dass wir bei der Datenverwaltung à la Cevisio bestehende Traumata vertiefen, und auch die Gefahren, dass unsere Datensammlungen in falsche Hände geraten, etwa von Geheimdiensten des Heimatlandes, sind groß. Auch Software-Unternehmen haben eine Verantwortung dafür, dass solche Gefahren gebannt werden. Wir sollten uns bewusst machen: Was heute an Flüchtlingen praktiziert wird, wird morgen vielleicht schon auf uns angewendet.

Herzlichen Glückwunsch zum BigBrotherAward 2018 in der Kategorie Verwaltung, Cevisio.

Thilo Weichert

EuGH: Facebook-Fanpagebetreiber mitverantwortlich für Nutzertracking

Der Gerichtshof der Europäischen Union (EuGH) hat mit Urteil vom 05.06.2018 bestätigt, dass die Betreiber einer Facebook-Fanpage – neben Facebook – datenschutzrechtlich dafür verantwortlich sind, dass Facebook Daten der Fanpage-Besuchenden zur Erstellung von Besuchsstatistiken erhebt (C-210/16).

Ausgangspunkt der Entscheidung ist ein seit 2011 anhängiger Verwaltungsrechtsstreit zwischen der von der

Industrie- und Handelskammer (IHK) Schleswig-Holstein betriebenen Wirtschaftsakademie Schleswig-Holstein GmbH und dem heute von Marit Hansen geleiteten Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD). Das Unternehmen vertrat die Auffassung, es dürfe eine Facebook-Fanpage betreiben, ohne sich darum kümmern zu müssen, ob Facebook das Datenschutzrecht einhält.

Das Urteil

Der EuGH stellte nun klar, dass diese Auffassung nicht mit europäischem Datenschutzrecht vereinbar ist: „Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien." (Rn. 40)

Datenschutzrechtlich verantwortlich ist, wer über die Zwecke und Mittel einer Verarbeitung personenbezogener Daten entscheidet. Der EuGH stellte fest, dass der Begriff des Verantwortlichen weit zu fassen ist, um einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten. Der Betreiber einer Facebook-Fanpage ist beteiligt an der Entscheidung über die Zwecke und Mittel der Verarbeitung personenbezogener Daten der Besucherinnen und Besucher seiner Fanpage. Er gestaltet sein Informations- und Kommunikationsangebot selbst und trägt damit zur Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage bei. Da Facebook ebenfalls die Zwecke und Mittel der Verarbeitung bestimmt, haben Facebook und Betreiber von Facebook-Fanpages die datenschutzrechtliche Verantwortlichkeit gemeinsam wahrzunehmen.

Der EuGH führt aus, dass ein Fanpage-Betreiber nicht bloßer Facebook-Nutzer ist, sondern als Verantwortlicher Facebook die Möglichkeit gibt, durch den Betrieb der Fanpage Cookies zu setzen, und mit Hilfe von durch Facebook zur Verfügung gestellten Filtern die Kriterien festzulegen, nach denen Statistiken erstellt werden. Für die Verantwortlichkeit ist nicht ausschlaggebend, dass ein Zugang zu den betreffenden personenbezogenen Daten besteht.

Zur Art der „Verantwortlichkeit" führt der EuGH in Rn. 43 Folgendes aus: „Klarzustellen ist, dass das Bestehen einer gemeinsamen Verantwortlichkeit, wie der Generalanwalt in den Nrn. 75 und 76 seiner Schlussanträge ausgeführt hat, aber nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure zur Folge hat, die von einer Verarbeitung personenbezogener Daten betroffen sind. Vielmehr können diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist."

Am 24.10.2017 hatte der Generalanwalt Yves Bot in seinem Schlussantrag in den zitierten Passagen Folgendes ausgeführt: „(75) Es ist auch darauf hinzuweisen, dass das Bestehen einer gemeinsamen Verantwortlichkeit keine gleichrangige Verantwortlichkeit bedeutet. Im Gegenteil können die verschiedenen für die Verarbeitung Verantwortlichen in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß einbezogen sein (vgl. in diesem Sinne Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010, S. 27). (76) Laut der Artikel-29-Datenschutzgruppe „[dient d]ie Möglichkeit einer pluralistischen Kontrolle ... zur Abdeckung der zunehmenden Zahl von Fällen, in denen verschiedene Parteien als für die Verarbeitung Verantwortliche handeln. Die Prüfung der gemeinsamen Kontrolle sollte in gleicher Weise erfolgen wie die Prüfung der ‚alleinigen' Kontrolle: Dabei sollte ein materieller und funktioneller Ansatz verfolgt werden, wobei der Schwerpunkt auf der Frage liegen sollte, ob mehr als eine Partei über die Zwecke und die wesentlichen Elemente der Mittel entscheiden. Die Beteiligung der Parteien an der Bestimmung der Zwecke und Mittel der Verarbeitung kann im Rahmen einer gemeinsamen Kontrolle jedoch verschiedene Formen aufweisen und muss nicht gleichmäßig verteilt sein" (Stellungnahme 1/2010, S. 39). Sind nämlich „mehrere Akteure an Entscheidungen beteiligt ..., kann ihre Beziehung sehr eng (z. B. vollständig übereinstimmende Zwecke und Mittel der Verarbeitung) oder eher locker sein (es stimmen z. B. nur die Zwecke oder nur die Mittel oder nur Teile davon überein). Daher sollten zahlreiche unterschiedliche Typologien für die gemeinsame Kontrolle betrachtet und ihre rechtlichen Folgen bewertet werden, wobei eine gewisse Flexibilität erforderlich ist, um der zunehmenden Komplexität der heutigen Gegebenheiten im Bereich der Datenverarbeitung Rechnung zu tragen (Stellungnahme 1/2010, S. 23 und 24)."

Der EuGH bestätigte in seinem Urteil zudem, dass das ULD entgegen den Entscheidungen der deutschen Vorinstanzen aufsichtsbehördliche Maßnahmen gegen den in Schleswig-Holstein ansässigen Betreiber einer Facebook-Fanpage richten durfte. Allein die Möglichkeit, aufsichtsbehördlich auf Facebook einzuwirken, schließt Maßnahmen gegen den mitverantwortlichen Anbieter einer Facebook-Fanpage nicht aus.

Reaktionen

Die Landesbeauftragte für Datenschutz Schleswig-Holstein Marit Hansen begrüßte das Urteil des EuGH: „Die Entscheidung hat meine Einschätzung bestätigt, dass es keine Verantwortungslücken im Datenschutz geben kann. Konkret bedeutet dies nun für alle Fanpage-Betreiber, dass zwischen ihnen und Facebook geklärt sein muss, welche Datenschutzpflichten sie selbst zu erfüllen haben und für welche Facebook zuständig ist. Dies gilt insbesondere für die Informationspflichten: Ohne Transparenz, wie die Daten über alle Nutzenden – d. h. Mitglieder und Nicht-Mitglieder von Facebook – verarbeitet werden, funktioniert dies nicht. Bei den Betroffenenrechten, z. B. dem Recht auf Auskunft oder Berichtigung, gilt: Jeder kann diese Rechte sowohl gegenüber dem Fanpage-Betreiber als auch gegenüber Facebook direkt geltend machen."

Hansen hält es für nötig, dass Fragen zur Datenschutz-Grundverordnung dem EuGH in Zukunft früher vorgelegt werden: „Für Rechtssicherheit ist eine schnelle gerichtliche Klärung essentiell. Gerichtliche Verfahren zu derarti-

gen Grundsatzfragen gehören auf die Überholspur. Ich bin davon überzeugt, dass einige Fälle von Datenmissbrauch – ich erinnere an Cambridge Analytica – hätten verhindert werden können, wenn bereits 2011 alle deutschen oder gar europäischen Fanpage-Betreiber die Datenschutzkonformität für ihre Angebote eingefordert hätten."

Der Bayerische Landesbeauftragte für den Datenschutz Thomas Petri empfahl öffentlichen Stellen, ihre Öffentlichkeitsarbeit bei Anbietern Sozialer Medien kritisch zu überprüfen: „Der Europäische Gerichtshof hat unmissverständlich klargestellt, dass der Betreiber einer Fanpage nicht dadurch von der Beachtung seiner datenschutzrechtlichen Pflichten freigestellt ist, dass er die von einem anderen Anbieter gestellte Plattform nutzt." Entweder müssten Soziale Medien sich an die in Europa geltenden Datenschutzvorschriften halten oder sie könnten nicht mitverantwortlich genutzt werden. „Mögliche Vorteile bei der Öffentlichkeitsarbeit rechtfertigen jedenfalls keine Datenschutzverstöße"

Marcus Schween, Rechtsvertreter der IHK Schleswig-Holstein, interpretierte das EuGH-Urteil entgegengesetzt: „Gegen einzelne Fanpagebetreiber vorzugehen ist daher unverhältnismäßig und rechtswidrig. Das sieht offenbar auch der EuGH so." Das Gericht habe dazu ausdrücklich klargestellt, dass sich die Datenschutzaufsicht unmittelbar an Facebook wenden kann. „Das ist sachgerecht, weil es wesentlich effektiver ist, datenschutzrechtliche Auseinandersetzungen direkt mit Facebook selbst zu führen. Lägen „tatsächlich Datenschutzverstöße vor, so kann allein Facebook diese abstellen – und das europaweit mit Wirkung für alle Nutzer und Fanpagebetreiber." Demgegenüber hätten Fanpagebetreiber schlicht keine Möglichkeit, auf die Datenverarbeitung von Facebook Einfluss zu nehmen. „Nach dieser Entscheidung rechnen wir damit, dass der Rechtsstreit beim Bundesverwaltungsgericht in Leipzig nach beinahe sieben Jahren beendet werden wird. Auch wenn es dann lange gedauert hat, freuen wir uns, für unsere Mitgliedsunternehmen in Schleswig-Holstein schlussendlich Rechtssicherheit erreicht zu haben."

Und Facebook? Das Unternehmen gab zum Urteil keinen Kommentar ab. Facebook-Chef Mark Zuckerberg hatte wenige Tage vor dem Urteil in der Anhörung vor dem Europäischen Parlament behauptet, dass Facebook DSGVO-konform sei.

Als Fanpagebetreiber wandte sich nach dem Urteil die Böll-Stiftung an Facebook und forderte gemäß Rn. 43 des Urteils den Abschluss einer Vereinbarung. Darauf antwortete für Facebook eine Anika mit folgender Mail: „Hallo Lukas, wir haben folgendes Messaging dazu. There are no immediate implications on your ability to operate Pages on Facebook. You can continue to use Facebook services as normal. As this case dates back to 2011 – prior to the GDPR coming into effect – die ECJ has clarified the legal framework which was applicable at that time. The case was about delineating the responsibilities of parties that provide online services, not about the legality of Facebook´s products. Furthermore, this ruling applies to internet services more broadly – not just Facebook. The case will now be referred back to the German court which will determine next steps. We ´ll work with partners and regulators in Europe to limit any potential impact on our services or the people and businesses that use them. And if necessary, we ´ll work with you and other Page admins on how to can comply with your obligations. Liebe Grüße Anika."

Übersetzung ins Deutsche: „Das Urteil hat keine direkte Auswirkungen auf Deine Fähigkeit, Facebook-Fanpages zu betreiben. Du kannst Facebook-Dienste weiterhin wie üblich nutzen. Da der Fall auf das Jahr 2011 – also vor dem Wirksamwerden der DSGVO – zurückgeht, legte der EuGH den damals gültigen rechtlichen Rahmen aus. Es ging um die Beschreibung der Verantwortlichkeiten der Parteien beim Erbringen von Webdiensten, nicht um die Rechtmäßigkeit der Facebook-Produkte. Zudem ist das Urteil nicht nur auf Facebook, sondern weiter gehend auf Internetdienste anwendbar. Der Fall wird nun zum deutschen Gericht zurückverwiesen, das die nächsten Schritte festlegen wird. Mit unseren Partnern und den Aufsichtsbehörden werden wir mögliche Auswirkungen für unsere Dienste oder die diese nutzenden Menschen oder Unternehmen begrenzen. Bei Bedarf arbeiten wir mit Dir und anderen Seiten-Administratoren zusammen, damit Du Deinen Verpflichtungen genügen kannst."

Rechtliche Schlüsse

Es ist irritierend, wie die IHK Schleswig-Holstein trotz der eindeutigen Formulierungen weiterhin jegliche Verantwortung der Wirtschaft für die Inanspruchnahme digitaler Plattformen zurückweist. Im Rahmen des Auswahlermessens nahm sich das ULD als Aufsichtsbehörde schon 2011 zurück und beschränkte sich auf die Durchführung eines „Musterverfahrens".

Facebook selbst spielt weiterhin auf Zeit: Das Unternehmen wird gegen alles, was ihm auferlegt werden wird, Rechtsmittel einlegen, insbesondere wenn es um die materiell-rechtliche Bewertung seiner Datenverarbeitung geht, also um die Grundlagen seines Geschäftsmodells.

Welche Anpassungsleistungen Facebook – und andere Internet-Plattformen bzw. -Dienste – erbringen werden, hängt ausschließlich vom öffentlichen und rechtlichen Druck ab, der nun ausgeübt wird. In einem hat Facebook Recht: Das EuGH-Urteil betrifft nicht nur dieses Unternehmen, sondern praktisch sämtliche Internetdienste. Eine Fokussierung des Drucks auf Facebook und zudem auf Google ist aber schon aus Ressourcengründen sinnvoll, aber auch, weil deren Geschäftsmodell am massivsten auf illegaler Datenauswertung basiert. Diese Fokussierung sollte durch alle möglichen Beteiligten erfolgen: Nichtregierungsorganisationen, Verbraucherzentralen, Betroffene, (Fach-)Öffentlichkeit und Aufsichtsbehörden. Spannend wäre, wenn sich deutsche Wettbewerber dieser US-Firmen fänden, die wegen Wettbewerbsverzerrung gegen die Internet-Giganten vorgingen. So würden datenschutzrechtliche Abmahnungen wenigstens Sinn machen. Doch diese Hoffnung dürfte angesichts der realen Marktmacht ein Traum bleiben.

Wie die Geschichte dieses Urteils fortgesetzt wird, ist völlig offen. Von Facebook eingefordert werden muss

nun als erstes die in Art. 26 DSGVO eingeforderte „Vereinbarung“ zwischen Facebook und seinen Fanpagebetreibern. Diese muss in „transparenter Form“ erfolgen, ist also zu veröffentlichen und muss den Anforderungen der Art. 12 ff. DSGVO genügen, d. h. muss in präziser, verständlicher, leicht zugänglicher Form und in „klaren und einfachen Sprache“ erfolgen. Die Vereinbarung muss Zwecke und Art der Verarbeitungen festlegen; d. h. Facebook muss gezwungen werden, Art und Ort der Erfassung, Speicherung und Auswertung der erfolgenden Verarbeitung offenzulegen. Nur auf dieser Grundlage kann dann auch festgelegt werden, wie und gegenüber wem die Betroffenen ihre Rechte geltend machen können, was letztlich auch in die Vereinbarung einfließen muss.

Facebook wird sich insofern zunächst verweigern. Dann stellt sich die Frage, wie das Unternehmen gezwungen werden kann, seinen Pflichten nach der DSGVO gegenüber den Fanpagebetreibern gerecht zu werden. Die Antwort darauf gibt Art. 79 Abs. 2 DSGVO. Dieser hat zwar vorrangig das Verhältnis von Betroffenen zu Verantwortlichen und Auftragsverarbeitern im Blick, gilt aber für sämtliche die DSGVO als Streitgegenstand betreffenden gerichtlichen Auseinandersetzungen. Da Facebook eine Niederlassung in Deutschland hat, sind nach dieser Regelung auf die Klage eines deutschen Fanpagebetreibers die deutschen Gerichte zuständig. Der hamburgischen Aufsichtsbehörde sind nach Art. 58 Abs. 2 lit. d DSGVO die für die Vereinbarung nötigen Informationen zur Verfügung zu stellen und ein Vorschlag für eine solche Vereinbarung zu machen. Auch ein Verbraucherschutzverband kann ein derartiges Verfahren nach § 2 Abs. 2 Nr. 1 UKlaG in Gang setzen.

Die materiell-rechtlichen Beschwerden, die Max Schrems in Irland vorgetragen hat und anlässlich der direkten Anwendbarkeit der DSGVO vertieft hat, sowie weitere anhängige Verfahren in Bezug auf rechtswidrige Datenverarbeitung durch Facebook müssen parallel weitergeführt werden. Es geht nicht anders, aber nötig sind jetzt erst recht die Offenlegung der Praktiken bei Facebook, deren öffentliche Thematisierung und viele rechtliche, aufsichtsbehördliche, zivilrechtliche und gerichtliche Verfahren (PM ULD, BayLfD, Betreiber von Facebook-Fanpages tragen Datenschutz-Verantwortung! v. 05.06.2018; Schulzki-Haddouti, EuGH: Betreiber von Facebook-Fanseiten sind für Datenschutz mitverantwortlich, www.heise.de 05.06.2018; PM IHK, EuGH äußert sich zu zentralen Fragen, www.ihk-schleswig-holstein.de Nr. 4086290).

Presseerklärung der DVD

Bonn, 29. Mai 2018

DVD: Sachsen-Anhalt Datenschutz-Entwicklungsland!?

Die Deutsche Vereinigung für Datenschutz e. V. (DVD) zeigt sich schockiert darüber, dass nach zwei vergeblichen Versuchen am 08. März auch beim dritten Wahlgang am 24. Mai 2018 sich der Landtag von Sachsen-Anhalt als unfähig erwies, einen neuen Landesbeauftragten für den Datenschutz zu wählen. Der Kandidat, der 49jährige Nils Leopold, wurde von der Grünen vorgeschlagen. Er erhielt 48 der 83 Stimmen des Landtags und verpasste damit auch im dritten Wahlgang um acht Stimmen die gesetzlich geforderte Zweidrittelmehrheit. Zuvor hatten sich außer den Regierungsfraktionen CDU, SPD und Grüne auch die Linken öffentlich zu Leopold bekannt, dessen fachliche Qualifikation von niemandem in Frage gestellt wurde. Selbst die AfD hatte ihren Abgeordneten die Wahl freigestellt.

Die Nichtwahl von Leopold erfolgte zu einem Zeitpunkt, zu dem der bisherige Landesbeauftragte schon mehr als ein Jahr kommissarisch das Amt fortführen musste. Ein Umsetzungsgesetz des Landes für die Datenschutzgrundverordnung, die seit dem Tag nach der Nichtwahl auch in diesem Bundesland direkt anwendbar ist, ist bisher (bis auf eine kleinere Änderung des Landesdatenschutzgesetzes bezogen auf die Datenschutzaufsichtsbehörde vom 06.05.2018) noch kein Thema im Landesparlament.

Der DVD-Vorsitzende Frank Spaeing kommentierte: „Das Trauerspiel um die Nichtwahl Leopolds zeigt ein weiteres Mal, welchen Stellenwert der Datenschutz für die Politik gemeinhin hat. Es ist nicht das erste Mal, dass ganz offensichtlich fachfremde Erwägungen den Ausschlag bei der Wahl für diese Funktion geben, dass Abgeordnete ihren Frust über eine schwierige Koalitionspolitik auf diese feige Art und zum Schaden des Datenschutzes zum Ausdruck bringen. Zwar redet alle Welt von der nötigen Digitalisierung; eine verantwortungsvolle Wahrnehmung dieser Gestaltungsaufgabe wird aber verweigert.“

Sein Stellvertreter Werner Hülsmann ergänzt: „Wenn das Land nicht jeden Kredit in Sachen digitaler Grundrechtsschutz verspielen möchte, sollte der Landtag in einer Schnellgesetzgebung die einfache Mehrheit für die Wahl des Datenschutzbeauftragten für ausreichend erklären und dann einen kompetenten Kandidaten oder eine solche Kandidatin wählen. Es ist absurd, dass für die Wahl des Ministerpräsidenten die einfache Mehrheit genügt, für die Wahl des weniger einflussreichen Chefs der Datenschutzaufsicht dagegen eine qualifizierte Zweidrittelmehrheit. Außer Sachsen-Anhalt kennt nur noch Niedersachsen dieses hohe Quorum, das auch dort zu massiven Zeitverzögerungen bei der Wahl für diese wichtige Kontrollfunktion führte.“

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Ulrich Kelber soll neuer BfDI werden

Der Bonner SPD-Bundestagsabgeordnete (MdB) Ulrich Kelber soll nach dem Willen der SPD neuer Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) werden und Andrea Voßhoff ablösen. Damit hätte erstmals ein Informatiker diesen Posten inne. Am 01.01.2019 will Kelber sein Mandat als Bonns direkt gewählter Bundestagsabgeordneter niederlegen, um seinen neuen Job in der Bonner Behörde anzutreten. Die Wahl soll zuvor im Dezember im Bundestag stattfinden. Die SPD hat in dieser Legislaturperiode das Vorschlagsrecht für die Besetzung. Die amtierende BfDI Andrea Voßhoff hatte bereits während der Jamaika-Verhandlungen 2017 gegenüber Mitarbeitenden sowie dem Bundesinnenministerium signalisiert, dass sie für eine zweite Amtszeit nicht zur Verfügung stehen werde.

Kelber ist Diplom-Informatiker und hat in den 90er-Jahren am GMD Forschungszentrum Informationstechnik und bis 2001 als Berater bei Comma Soft gearbeitet. Er hatte sich in der vergangenen Legislaturperiode als Parlamentarischer Staatssekretär für Verbraucherschutz, Mietrecht und Digitales bereits für einen besseren Datenschutz eingesetzt, allerdings im Rahmen der Großen Koalition nur mit mäßigem Erfolg. Er stimmte zwar für die Wiedereinführung der Vorratsdatenspeicherung, gleichwohl lehnte er die Online-Durchsuchung und den Einsatz von Staatstrojanern ab. Als „gläserner MdB" legte er seine Einkünfte offen.

Kelber wird eine vergleichsweise gut ausgestattete Behörde übernehmen. Die Juristin und ehemalige CDU-Parlamentarierin Voßhoff konnte in den letzten Haushaltsverhandlungen erhebliche Stellenzuwächse erreichen, so dass sich die Zahl der Mitarbeitenden der BfDI-Dienststelle seit ihrem Amtsantritt 2015 fast verdoppelte. Der Grund für die Personalaufstockung war nicht nur der stete Aufgabenzuwachs. Die Landesdatenschutzbehörden erhielten bei ähnlichem Aufgabenzuwachs erheblich weniger Personalmittel. Vor allem die unionsinternen Überlegungen, alle Landesbehörden zugunsten einer großen zentralen Bundesbehörde abzuschaffen, dürften für die Zustimmung der Union in den Haushaltsverhandlungen eine Rolle gespielt haben. Unterstützt werden diese Pläne in der aktuellen Regierung unter anderem von der neuen Digitalstaatssekretärin Dorothee Bär. Voßhoff konnte erreichen, dass der Bund im Europäischen Datenschutzausschuss (EDSA), der Nachfolgeeinrichtung der Artikel-29-Gruppe, als erster Vertreter Deutschlands fungiert. Aus den Landesbehörden wird der Stellvertreter benannt, wobei das jeweils diensthabende Land vom Bundesrat bestimmt werden wird. Der Bund führt außerdem eine Geschäftsstelle, welche die europäischen Aktivitäten koordinieren wird (Schulzki-Haddouti, Ein Informatiker als Bundesdatenschutzbeauftragter: SPD schlägt Ulrich Kelber vor, www.heise.de 17.03.2018).

Bund

Digital-Staatsministerin Bär: Keine Ahnung vom Datenschutz

Wenn die von der CSU benannte neue Digitalstaatsministerin Dorothee Bär gefragt worden wäre, ob sie wüsste, was Datenschutz ist, hätte sie sicher nicht ausdrücklich zugegeben, dass sie davon keine Ahnung hat. Doch in unserer populismusverseuchten Politik lassen sich solche Botschaften sogar positiv verpacken. Dies versuchte Bär nach ihrer Nominierung in einem Interview mit der BILD-Zeitung, als sie dem Journalisten beipflichtete, der meinte „der gute alte Datenschutz" würde Chancen im Gesundheitsbereich verhindern. Sie ergänzte: „Wir brauchen deshalb endlich eine smarte Datenkultur vor allem für Unternehmen. Tatsächlich existiert in Deutschland aber ein Datenschutz wie im 18. Jahrhundert."

Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein, erwiderte hierauf: „Zum Glück ist es eben nicht so wie im 18. Jahrhundert, als Datenschutz ein Fremdwort war und sich die Idee der Grundrechte noch nicht weithin durchgesetzt hatte. Auch die Unterstellung, Datenschutz sei ein Verhinderer der Digitalisierung, ist falsch. Wichtig ist aber, dass die Grundrechte von Anfang an mitbedacht und in die entwickelten Lösungen eingebaut werden. Datensparsamkeit und Zweckbindung sind keineswegs überholt, sondern gehören weiterhin zum Fundament für eine demokratische Informationsgesellschaft. Datenschutz-Grundsätze sind also nicht veraltet, sondern müssen in die smarte Technik Eingang finden, um den Risiken durch Datenkraken und Sicherheitslücken entgegenzuwirken. Die Wirtschaft, Forschung und Politik sind gefordert, solche innovativen Lösungen voranzubringen. Der Datenschutz des 21. Jahrhunderts in unserer Welt, in der bald alles mit allem vernetzt wird, muss in Produkten und Infrastrukturen endlich zur Selbstverständlichkeit werden. Ich begrüße es, wenn das Digitalisierungsministerium eine smarte Datenkultur im Sinne der Grundrechte fördert."

Ähnlich sachlich argumentierte die Linken-Vorsitzende Katja Kipping: „Inzwischen wissen Facebook und Co mehr über die Menschen als jeder Geheimdienst". Den Herausforderungen der Digitalisierung könne nicht begegnet

werden, „indem wir Grundrechte und Datenschutz als unmodern abtun“.

Auch der Parlamentarische Staatssekretär im Bundesjustizministerium und designierter künftiger Bundesdatenschutzbeauftrater Ulrich Kelber (s. o.), kritisierte Bärs Äußerungen zum Datenschutz. Datenschutz sei Schutz von Grundrechten: „Das kommt nie aus der Mode und ist in Zeiten umfassender digitaler Datenerhebung und -analyse dringender als je zuvor.“ Dies bestätigten auch zahlreiche Urteile des Bundesverfassungsgerichts. „Es ist mir unerklärlich, wie Frau Bär das als 18. Jahrhundert abtun kann.“ Irritierend sei überdies, so Kelber, „dass Frau Bär anscheinend nicht realisiert hat, dass ab Mitte Mai außerdem in der gesamten Europäischen Union ein neues, modernisiertes Datenschutzrecht gilt, dass genau diesen Schutz der Grundrechte in den Mittelpunkt rückt“. Falsch sei die Behauptung Bärs, der deutsche Datenschutz würde einer Nutzung von Daten etwa im Gesundheitsbereich entgegenstehen. „Der Abgleich von Patientendaten mit einer Datenbank ähnlicher Fälle scheitert natürlich nicht am Datenschutz. Wenn Frau Bär abseits von Floskeln wie smart konkrete Vorschläge hat, kann man darüber sprechen, aber so ist das eine Luftnummer.“

So sehr Hansen, Kipping und Kelber Recht haben, so wenig verfangen ihre Argumente bei einer zur „Staatsministerin“ aufgeblasenen Staatssekretärin, der es darum geht, heiße Luft zu verbreiten, etwa wenn sie erklärt, den Unternehmen helfen zu wollen, „Champions League zu spielen, Weltmeister zu sein“. Sie wolle dabei „ein Taktgeber“ sein. Ihr gehe die Digitalisierung „viel, viel zu langsam“. Jetzt entscheide sich die Zukunft des Landes: „Wir sind im Moment eine sehr erfolgreiche Industrienation. Das heißt aber nicht, dass wir auch eine erfolgreiche Digitalnation bleiben.“ Digitalisierung müsse für alle Politiker, Bürger und Unternehmen „das Topthema Nummer Eins“ sein.

Politik gemäß dieser Denke betreibt die Bundesregierung schon lange, angeführt von Bundeskanzlerin Angela Merkel (CDU) und dem zeitweiligen Wirtschaftsminister und Vizekanzler Sigmar Gabriel (SPD) und sekundiert von einem Alexander Dobrindt (CSU), wie diese z. B. auf vergangenen IT-Gipfeln verlautbaren ließen. Auch die FDP, von der man nach ihrer Wahlschlappe 2013 hoffen konnte, sie würde sich auf ihre bürgerrechtlichen Wurzeln besinnen, plakatierte zur Bundestagswahl 2017 den Schlachtruf ihres Frontmanns Christian Lindner „Digital first, Bedenken second“.

Dass Digitalisierung eine politische Gestaltungsaufgabe ist, wird von der Politik bis heute entweder nicht erkannt oder dies ist wegen mangelnder Popularität kein politisches Thema. Die personelle Besetzung des Bundeskabinetts – auch jenseits der Digitalisierungs-Staatsministerin ohne Personal und Ahnung – lässt nichts Gutes ahnen („Angriff auf Datenschutz“ SZ 07.03.2018, 5; Neuerer, SPD-Staatssekretär attackiert künftige Digitalministerin für Aussagen zum Datenschutz, www.wiwo.de 07.03.2018; ULD PE v. 06.03.2018: „Zukunftsweisender Datenschutz in Deutschland und Europa Staat „wie im 18. Jahrhundert“; So will Dorothee Bär Deutschland digitalisieren, www.faz.net 06.03.2018).

Bund

Bundesgesundheitsminister Spahn hält nichts vom Datenschutz

Der neue im Bundeskabinett zuständige Gesundheitsminister Jens Spahn (CDU, 37 Jahre alt, seit 15 Jahren im Bundestag), war zwar direkt vor dieser Nominierung etwas länger als ein Jahr Staatssekretär im Bundesfinanzministerium, doch engagierte er sich zuvor und auch während dieser Zeit in der Gesundheitspolitik und zeigte sich kritisch gegenüber dem Datenschutz. September 2016 veröffentlichte er gemeinsam mit dem ehemaligen Chef des Hamburger Uni-Klinikums Eppendorf Jörg Debatin sowie Markus Müschenich, Mitgründer des Bundesverbands Internetmedizin und Mitglied der Arbeitsgruppe „Telemedizin“ in der Bundesärztekammer, im konservativen Herder-Verlag das Buch „App vom Arzt – Bessere Gesundheit durch digitale Medizin“. Eine zentrale Aussage des Buchs ist: „Datenschutz ist was für Gesunde“ Denn insbesondere kranke Menschen würden von einem vermehrten Datenaustausch im Gesundheitswesen profitieren.

Um ihre Vision von der Versorgung der Zukunft zu erläutern, führen die Autoren folgende Situation an: Man wacht mitten in der Nacht mit Herzrasen auf. „Welch ein Segen wäre es da für Sie, für Ihren ruhigen Schlaf und auch Ihren Partner oder Ihre Partnerin, wenn Sie die Symptome einfach in eine App eingeben könnten, die Ihre Krankengeschichte kennt und mit den akuten Beschwerden abgleicht und Ihnen so in Sekundenschnelle entweder akute Maßnahmen empfiehlt oder Sie direkt per App mit einem Arzt verbindet, der Ihnen sofort zuhört.“ Dem Buch zufolge sterben in Deutschland pro Jahr mehr Menschen an falsch aufeinander abgestimmten Medikamenten als im Straßenverkehr. Das ließe sich vermeiden, wenn Ärzte und Apotheker mehr über die Einnahmegewohnheiten der PatientInnen wüssten. „Wenn Ihr Medikationsplan digital verfügbar ist, in dem mit Ihrer Zustimmung festgehalten wird, welche Medikamente Sie wann und wie oft nehmen müssen und welches Behandlungsziel damit verfolgt wird, dann können diese Entscheidungen blitzschnell auf einer viel besseren Basis getroffen werden.“

Das Werk sieht eine Zukunft in der „personalisierten Arzneimittelversorgung“: „Vielleicht erleben wir bald das Ende der Arzneimittel, wie wir sie heute kennen.“ Denn heutzutage würden Medikamente nach dem Motto „One size fits all“ ausgegeben. Wenn aber mit Hilfe der Datensätze anderer PatientInnen zuvor abgeglichen würde, ob es ähnliche Behandlungsfälle gab, in der die Therapie erfolgreich verlief, dann könnten personalisierte und einmalige Wirkstoff-Zusammenstellungen produziert werden.

Für alle im Buch vorgestellten Versorgungsverbesserungen durch eine digitalisierte Medizin sei aber ein „weniger verkrampftes Verhältnis zum Umgang mit den Daten“ nötig, so die Autoren. Ziel sei es, die Sensibilität für das Bedürfnis nach Datenschutz und -sicherheit zu verlieren: „Daten haben also einen weitaus größeren Nutzen als nur den, dass Unternehmen uns personalisierte Werbung zukommen lassen kön-

nen. Sie sind der Rohstoff der Zukunft für ein hochindustrialisiertes Land wie Deutschland."

Wie Spahn seine Vorstellungen von der Digitalisierung der Medizin umsetzen wird, muss sich zeigen. Im schwarz-roten Koalitionsvertrag heißt es: „Es wird sichergestellt, dass die Datenspeicherung den strengen Anforderungen des Datenschutzes unterliegt." Selbst „ein Verbot des Versandhandels mit verschreibungspflichtigen Arzneimitteln" ist dort vorgesehen. Damit würde das Geschäft des Online-Händlers Doc Morris durchkreuzt, wo Spahns Freund Max Müller im Vorstand sitzt. Spahn und Müller hatten sich 2006 gemeinsam an der Lobbyagentur Politas beteiligt, die ihren Kunden „gute persönliche Kontakte" im politischen Berlin versprach („Datenschutz ist was für Gesunde", www.deutsche-apotheker-zeitung.de, 10.06.2016; Ludwig, Der Anti-Gröhe, SZ 01.03.2018, 6).

Bund

CDU und FDP nutzen Post-Daten für Wahlkampfzwecke

Es war offenbar kein Aprilscherz, als die „Bild am Sonntag" am 01.04.2018 berichtete, dass die Post Direkt, eine Tochter der Deutschen Post AG, im Bundestagswahlkampf zugunsten der CDU und der FDP Kundendaten für Werbezwecke eingesetzt hat. Demgemäß verkauft der ehemalige Staatskonzern seit 2005 Daten an Parteien zu Wahlkampfzwecken. 2017 sollen CDU und FDP jeweils einen fünfstelligen Betrag für straßengenaue Analysen gezahlt haben.

Ein CDU-Sprecher teilte mit, man habe im Wahlkampf eine Massenpostsendung bei der Post Direkt in Auftrag gegeben. Dabei seien keine Daten an die CDU übermittelt oder über Einzelhaushalte gekauft worden. Die Post habe für den Haustürwahlkampf eine statistische „CDU-Wahlwahrscheinlichkeit" für Straßenabschnitte geliefert. Dazu habe man Zugriff auf eine Kartenansicht erhalten. Es seien vollkommen anonymisierte Daten verwendet worden, ein Personenbezug sei nicht herstellbar gewesen. Der Zugang zur Datenbank sei nach der Wahl beendet worden. Thomas Jarzombek, für Digitales in der CDU-Bundestagsfraktion zuständig, warnte vor Hysterie und davor, die Post mit Facebook gleichzusetzen: „Es gibt personenbezogene Daten, das sind die, die Facebook erhebt. Dann gibt es noch pseudonymisierte Daten und anonymisierte Daten." Bei der Post gehe es lediglich um letztere. Die könne man nicht zu einzelnen Personen zurückverfolgen. Zum Fall Cambridge Analytica, bei dem mutmaßlich illegal Daten von 50 Millionen Facebook-Nutzenden abgeschöpft worden waren, hatte er erklärt: „Es droht ein Riesenskandal." Mit Blick auf die eigene Datennutzung meinte er, man dürfe keine Ablenkungsgefechte führen, sodass Facebook am Ende sagen könne, das machten alle: „Das machen eben nicht alle. Wir sind auf dem Weg in eine Datenökonomie." Die Verarbeitung unproblematischer Daten sei lebensnotwendig für die Wirtschaft: „Es darf nicht der Eindruck entstehen, Daten zu verarbeiten wäre etwas Schlechtes."

Der Parlamentarische Geschäftsführer der FDP-Bundestagsfraktion, Marco Buschmann, schrieb auf Facebook, die von der Post erworbenen Daten seien vollständig anonymisiert gewesen und im Einklang mit dem Datenschutzrecht bearbeitet worden. Als Datenschutzpartei habe man darauf geachtet, dass keine personenbezogenen Daten verwendet wurden. Die Daten hätten zudem ausschließlich einen Wahrscheinlichkeitswert geliefert, „einen möglichen FDP-affinen Wähler anzutreffen".

Gemäß einem Sprecher der Post Direkt würden „personenbezogene Daten bei strikter Einhaltung des Bundesdatenschutzgesetzes" verarbeitet. Dargestellt worden seien keine personenbezogenen Daten, sondern nur statistische Wahrscheinlichkeitswerte. Die Daten bezögen sich somit nicht auf einzelne Haushalte. Die Firma sei unter Aufsicht des Bundesbeauftragten „über die Jahre regelmäßig überprüft worden". Die Daten bezögen sich auf sogenannte Mikrozellen, die statistisch 6,6 Haushalten entsprechen. Anke Domscheit-Berg, netzpolitische Sprecherin der Linken im Bundestag, kritisierte die Praxis: „Eine Weitergabe dieser privaten Daten muss ohne ausdrückliche Zustimmung verboten sein."

Gemäß einer Werbebroschüre der Post-Tochter mit Stand März 2018 stehen dem Unternehmen für circa 20 Millionen Häuser mit rund 34 Millionen Haushalten in Deutschland mehr als eine Milliarde Einzelinformationen zur Verfügung. Sie besitze Daten zu 85% aller Haushalte in Deutschland, darunter Angaben zu Kaufkraft, Bankverhalten, Geschlecht, Alter, Bildung, Wohnsituation, Familienstruktur, Wohnumfeld und Pkw-Besitz. Wer eine Adresse hat, landet automatisch in den Post-Datenbanken. Um die Weitergabe dieser Daten zu verhindern, muss der Nutzung schriftlich widersprechen.

Angaben zu politischen Präferenzen sind sensitive Daten gemäß § 3 Abs. 9 BDSG (Bundesdatenschutzgesetz), auch wenn es sich nur um Wahrscheinlichkeitsangaben handelt. Deren Verarbeitung für Werbezwecke war zum Verarbeitungszeitpunkt nicht gemäß § 28 Abs. 3 BDSG zulässig; vielmehr ist § 28 Abs. 6-9 BDSG anwendbar, wonach keine entsprechende Legitimation vorliegt. Insbesondere gilt auch § 28 Abs. 9 BDSG nicht, der auch für politische Parteien anwendbar ist, da eine „Erforderlichkeit" nicht besteht. Diese Regelung bezieht sich v. a. auf Mitglieder und InteressentInnen und nicht auf politisches Direktmarketing.

Zentral für die Bewertung ist also, ob, wie Post Direkt, FDP und CDU behaupten, hier ein Personenbezug besteht oder nicht. Dies ist zunächst davon abhängig, wie detailliert die Profile waren. Bei Mikrozellen mit statistisch 6,6 Haushalten im Straßenzug wird es oft vorkommen, dass auch nur ein Haushalt erfasst wird, so dass sich schon hieraus ein Personenbezug ergibt. Wurden zusätzlich zu den politischen Präferenzen weitere Daten (Kaufkraft, Alter, Bildung) einbezogen, dürfte zusätzlich fraglich sein, dass selbst bei einer Aggregierung der politischen Präferenz auf Straßenabschnitte eine Anonymisierung vorliegt. Keine Anonymität liegt in jedem Fall vor, wenn die Wahrscheinlichkeitsdaten (z. B. CDU-Wahlwahrscheinlichkeit) wieder einem personenbezogenen Datum (Adresse) zugeordnet wurden. Dies ist bei Massenpostsendungen zwangsläufig der Fall.

Gemäß den Pressedarstellungen wurden die Daten von Post Direkt im sog.

Lettershop-Verfahren eingesetzt. Der Rechtsverstoß läge dann vorrangig bei der Post Direkt. Bestand auch Zugang zu den Daten für die Parteien und haben sie diese für direkte Ansprachen, z. B. Haustürbesuche verwendet, dann sind auch die Parteien im datenschutzrechtlichen Sinn verantwortlich und hätten sich direkt rechtswidrig betätigt.

Von wenig Datenschutzkenntnissen zeugte das Statement des Postsprechers auch insofern, dass er auf die dauernde Kontrolle durch den Bundesdatenschutzbeauftragten hinwies. Dabei ist ihm offenbar entgangen, dass das Amt derzeit eine Frau innehat, die überhaupt nicht für die Post Direkt zuständig ist. Die Post Direkt ist ein Adresshändler, kein Postunternehmen, und unterliegt der Datenschutzkontrolle der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW).

Tatsächlich ließ die LDI NRW, Helga Block, umgehend mitteilen, dass ihre Behörde eine Prüfung begonnen hat, ob der Adresshandel von Post Direkt im Wahlkampf im Einklang mit dem Bundesdatenschutzgesetz stehe. Das Unternehmen werde innerhalb weniger Tage einen Fragenkatalog der Datenschutzbehörde erhalten, berichtete der LDI-Sprecher Nils Schröder. Das Prüfverfahren werde voraussichtlich etwa vier Wochen dauern; die Parteien seien zunächst nicht gefragt. Die Datenschutzbehörde empfahl zudem allen VerbraucherInnen, sich bei Post Direkt in Troisdorf zu erkundigen, was über sie gespeichert wurde.

Für das Direktwerbeverfahren bei Wahlen hat das deutsche Recht in den Meldegesetzen eine Regelung geschaffen, die politischen Parteien kurz vor der Wahl Adressdaten nach Alter aggregiert und ohne Wahlpräferenzen über die Meldebehörden bereitstellt. Würde man die Praxis der Post Direkt erlauben, so würden die strengeren Regeln des Melderechts umgangen. Diese strengen Regeln gelten schon seit langem. Sie sollen Wahlmanipulationen, wie sie gerade in den USA und GB bekannt wurden, verhindern (Deutsche Post verteidigt Datengeschäfte, www.spiegel.de 01.04.2018; Rossbach, Post als Wahlkampfhelfer, SZ 03.04.2018, 5; Wilkens, Datenschutzbehörde prüft Adresshandel mit Post-Daten im Bundestagswahlkampf, www.heise.de 03.04.2018).

Bund

Verfassungsbeschwerde gegen eGK-Markierung von chronisch Kranken

Der Verein Patientenrechte und Datenschutz e.V. unterstützt eine Beschwerde beim Bundesverfassungsgericht (BVerfG) eines IT-Ingenieurs, mit der sich dieser gegen die Kennzeichnung chronisch Kranker auf der elektronischen Gesundheitskarte (eGK) wendet. Nach Ansicht des Vereinsvorsitzenden Jan Kuhlmann, der zugleich den Ingenieur anwaltlich vertritt, ist diese Speicherung illegal. Alle Daten, die auf der eGK gespeichert werden dürfen, seien im Sozialgesetzbuch V aufgelistet. Dazu gehöre nicht die Kennzeichnung der Teilnahme an Behandlungsprogrammen der Krankenkassen für chronische Krankheiten. Solange Krankenkassen und Ärzteverbände diese unzulässige Datenspeicherung betrieben, verlangt der Kläger für seine Arztbesuche Papier-Ersatzbescheinigungen, wie sie Versicherte z. B. nach einem Umzug kurzfristig erhalten.

Der Kläger ist derzeit kein Teilnehmer in einem Chronikerprogramm. Trotzdem sieht er sein Arztgeheimnis und sein Recht auf Datenschutz schon jetzt gestört: „Ich muss ja bei allem, was ich meinem Arzt anvertraue, überlegen, in welcher Form es – jetzt oder irgendwann später – gespeichert und weitergegeben wird." Über 7 Millionen gesetzlich Krankenversicherte nehmen an „Disease Management Programmen" (DMP) teil, die es z. B. für Diabetes, koronare Herzkrankheit und COPD, den sogenannten Raucherhusten, gibt. Auf der eGK wird dafür ein Kennbuchstabe gespeichert. Welcher Buchstabe für welche Krankheit steht, ergibt sich aus einem öffentlichen Schlüsselverzeichnis, das z. B. bei Wikipedia nachzulesen ist. Das Landessozialgericht Baden-Württemberg hielt die Speicherung des Kennzeichens auf der Karte für rechtswidrig, umging aber eine Entscheidung in der Sache, weil der Kläger nicht persönlich betroffen sei. Der Kläger geht gegen die Klagerückweisung mangels Klagebefugnis vor, mit der Behauptung, dass das in vergleichbaren Fällen vom BVerfG schon anders entschieden worden wäre.

Über 80 % der Menschen in Deutschland sind in der gesetzlichen Krankenversicherung (GKV), die Mehrzahl davon hat eine eGK, die sie bei Arztbesuchen regelmäßig vorlegen müssen. Die DMP-Kennzeichnung geht auf Vorgaben der Krankenkassen und der Ärzteverbände zurück. Danach ist das DMP-Kennzeichen Teil der Versicherten-Stammdaten, die auf der eGK gespeichert und ab 2018 online zwischen Arztpraxen und Krankenkassen abgeglichen werden sollen. Die Gematik ist eine GmbH zur elektronischen Vernetzung des Gesundheitswesens, an der Krankenkassen, Krankenhaus- und Ärzteverbände beteiligt sind. PatientInnen haben hier keine Mitspracherechte. Dem versucht der Verein Patientenrechte und Datenschutz e.V. abzuhelfen, der die digitale Vernetzung des Gesundheitswesens aus Patientensicht kritisch begleitet (Verein Patientenrechte und Datenschutz, Kennzeichnung chronisch Kranker auf Elektronischer Gesundheitskarte – Verfassungsbeschwerde eingelegt, 20.03.2018).

Bundesweit

Aufsichtsbehörden benötigen mehr Ressourcen

Die neue europäische Datenschutz-Grundverordnung (DSGVO) wird nicht nur für Unternehmen, sondern auch für die Aufsichtsbehörden eine große Belastungsprobe werden. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Andrea Voßhoff, erklärte: „Besonders herausfordernd ist dabei schon jetzt die starke Beratungsnachfrage von Behörden und Unternehmen hinsichtlich der Umsetzung des neuen Rechts". Marit Hansen, Datenschutzbeauftragte von Schleswig-Holstein, sieht hierbei ein nicht kalkulierbares Risiko. „Die große Unbekannte ist das wohl deutlich steigende Aufkommen von Beschwerden, Beratungsersuchen und Gerichtsprozessen. Hier kann es sein, dass schon nach kurzer Zeit Aufsichtsbehörden Alarm schlagen müssen,

weil ihre Ausstattung nicht ausreicht und im Haushalt des Landes nachgelegt werden muss." Ein Rechtsgutachten im Auftrag des Hamburger Datenschützers Johannes Caspar weist einen künftigen Mehrbedarf von über 20 Stellen für die durchschnittliche Landesbehörde aus: „Das ist mehr als eine Reihe von Behörden derzeit an Personen überhaupt beschäftigt". Einige Mitgliedstaaten sowie der Bund und einige Länder hätten ihre Behörden personell für die neuen Aufgaben bereits aufgestockt oder entsprechend Stellen in den Haushaltsplänen ausgewiesen, andere aber noch nicht. Zwar bereiteten sich die Behörden seit Monaten auf die neuen Datenschutzregeln vor. Die neuen Arbeitsabläufe müssten aber „erst einmal eingeübt werden". Hierfür sei eine „auskömmliche Ausstattung" unverzichtbar. SpezialistInnen für die neuen Aufgaben sind aber nur schwer zu finden. Dies bestätigt auch Hansen: „Der Arbeitsmarkt für ausgebildete Datenschutzexperten, die Recht und Technik im Blick haben und möglichst Erfahrungen aus der Praxis mitbringen, ist weitgehend leergefegt". Caspar sieht weitere Probleme auf die Aufsichtsbehörden zukommen, sollte der Vollzug der Datenschutz-Grundverordnung nicht überall gleich erfolgen. „Es ist klar, dass allein die Vereinheitlichung des Rechts wenig bewirkt, wenn das Recht in jedem Mitgliedstaat anders angewendet wird". Der Effekt wäre: Unternehmen müssten „am Ort der laxen Auslegungspraxis selbst bei schweren Datenschutzverstößen nichts befürchten". Die „einheitliche Architektur der Datenschutzaufsicht" sei daher eines der wichtigsten Anliegen der DSGVO (Aufsichtsbehörden fürchten Überforderung durch EU-Datenschutz, www.fuldainfo.de 15.02.2018).

Bundesweit

Erpresser drohen mit Intim-Videos

In einer Erpressungswelle versuchen Kriminelle seit April 2018 die Scham ihrer Opfer auszunutzen. In einer E-Mail behaupten sie, mit Hilfe eines Trojaner per Webcam das Opfer während des Konsums pornografischer Videos gefilmt zu haben. Damit die Aufnahmen nicht verbreitet werden, sei ein Betrag von 500 Euro fällig:

„** xxx@yyy.de, Ihr Leben kann zerstört werden **

Guten Tag,

Masturbieren ist natürlich normal, aber wenn deine Familie und Freunde davon zeugen, ist es natürlich eine große Schande.

Ich habe dich eine Weile beobachtet, weil ich dich in einer Werbung auf einer Porno-Webseite durch einen Virus gehackt habe.

Wenn Sie das nicht wissen, werde ich es erklären. Ein Trojaner gibt Ihnen vollen Zugriff und Kontrolle über einen Computer (oder ein anderes Gerät). Das bedeutet, dass ich alles auf Ihrem Bildschirm sehen und Ihre Kamera und Ihr Mikrofon einschalten kann, ohne dass Sie es bemerken. So habe ich auch Zugang zu all deinen Kontakten.

Ich habe ein Video gemacht, das zeigt, wie du auf der linken Bildschirmhälfte masturbierst und auf der rechten Hälfte siehst du das Video, das du gerade angesehen hast. Auf Knopfdruck kann ich dieses Video an alle Kontakte Ihrer E-Mail und Social Media weiterleiten.

Wenn Sie dies verhindern möchten, überweisen Sie einen Betrag von 500 EUR auf meine Bitcoin-Adresse.

Schritt 1: Gehen Sie zu coinbase.com und erstellen Sie ein Konto.

Schritt 2: Bestätigen Sie Ihr Konto mit Ihrem Reisepass oder Personalausweis.

Schritt 3: Zahlen Sie das Geld auf Ihr Coinbase Bitcoin Konto über Ihre Kreditkarte oder Ihr Bankkonto ein.

Schritt 4: Schicken Sie die Münzen an die unten angegebene Bitcoin-Adresse:

1AipqebsiDBYKrhyFKagVoj1zBnwg2nq3s

Sobald die Zahlung eingegangen ist, lösche ich das Video und du wirst nie wieder von mir hören. Ich gebe Ihnen 3 Tage, um die Zahlung zu machen. Danach wissen Sie, was passiert. Ich kann es sehen, wenn Sie diese E-Mail gelesen haben, damit die Uhr jetzt tickt.

Es ist Zeitverschwendung, mich an die Polizei zu melden, da diese E-Mail weder in irgendeiner Form noch in meiner Bitcoin-Adresse nachverfolgt werden kann. Ich mache keine Fehler. Wenn ich feststelle, dass Sie einen Bericht eingereicht oder diese Nachricht an jemand anderen weitergegeben haben, wird das Video sofort verteilt.

Grüße!"

Auch wenn der geschilderte Sachverhalt technisch möglich wäre, handelt es sich hier zweifelsfrei um Fakes. Die E-Mails sind vor allem daran als Fälschungen zu erkennen, dass sie keinen konkreten Bezug zum Empfänger herstellen. In den aktuellen Kampagnen wird nicht einmal dessen Name verwendet. Erpresser mit echtem Drohpotential würden darüber hinaus ihre Forderung etwa durch Bilder untermauern, die keinen Zweifel daran lassen, dass sie die angeblichen Videos besitzen. Ist das nicht der Fall, können solche Erpresser-Mails ignoriert werden. Dennoch sollten sie der Polizei zur Anzeige gebracht werden verbunden mit der Übermittlung der Mail-Metadaten, so dass von den Ermittlern Rückschlüsse auf die zumeist ausländische Herkunft und auf die Täter möglich werden.

Als Empfehlung an alle, die sich vor Angriffen in die Intimsphäre schützen wollen, gilt: Deaktivieren Sie Kameras und Mikrophone. Überkleben Sie die Kamera auf ihrem Rechner, wenn Sie diese nicht benötigen. Und sollte es Hinweise geben, dass die in einer solchen Erpressungsmail enthaltene Drohung real ist, dann sollte in jedem Fall die Polizei eingeschaltet werden (Wilkens, Mail-Erpresser wollen Bitcoin: „Masturbieren ist natürlich normal, aber...", www.heise.de 04.05.2018).

Baden-Württemberg

Datenschutzbeauftragter fordert Nachbesserungen bei Windows 10

Der baden-württembergische Landesdatenschutzbeauftragte Stefan Brink fordert Microsoft auf, Windows 10 hinsichtlich ungeklärter Datentransfers „schleunigst nachzubessern". Längst bekannte Sicherheitsbedenken sind noch immer nicht ausgeräumt. Die Bürostandardsoftware in deutschen Behörden wird von Microsoft gestellt.

Trotz Sicherheitsbedenken wird teilweise bereits Windows 10 verwendet. Obwohl die Online-Services vollständig deaktiviert sind, werden dabei weiterhin einige verschlüsselte Datensätze an Microsoft übermittelt. Die BITBW als IT-Dienstleisterin für die Landesverwaltung in Baden-Württemberg hat ungeachtet der offenen Sicherheitsfragen unter anderem die Landesdatenschutzbehörde bereits mit Windows 10 ausgestattet.

Brink forderte Ende März 2018 Microsoft mit Blick auf die bekannt gewordenen Sicherheitslücken auf, „schleunigst nachzubessern und sich spätestens ab Ende Mai an die Datenschutz-Grundverordnung zu halten“. Die Systemadministratoren der betroffenen Systeme sollen bis dahin „durch entsprechende Grundeinstellungen dafür sorgen, dass möglichst wenig übertragen wird“. Was den Einsatz von Windows 10 im eigenen Haus anbelangt, erklärte Brink, dass die dort eigengenutzte Hard- und Software zwar kontinuierlich geprüft und bewertet werde, dass es „jedoch keine generelle Freigabe von Produkten mit verbindlicher Wirkung für die Verwaltung insgesamt“ gebe. Mit Blick auf die BITBW sagte er, dass er allerdings den Einsatz problematischer Produkte beanstanden und damit deren fortgesetzter Nutzung entgegentreten könne – „ab Mai 2018 sogar mit verbindlicher Wirkung“.

Brink stellte die rechtlichen Anforderungen an die öffentliche Beschaffung klar: „Ein Dienstleister, der diesen Anforderungen nicht genügen kann oder will, scheidet künftig aus dem Kreis derjenigen aus, mit denen ein datenschutzrechtlich Verantwortlicher kooperieren kann.“ Er hat dabei nicht nur das eigene Haus im Blick und betonte, dass „jeder Nutzer von Windows 10, wie auch anderen Betriebssystemen und Anwendungen, die volle Kontrolle über seine Daten haben muss“. Es müsse „volle Transparenz bezüglich der übertragenen Daten herrschen und der Anwender muss jede Übertragung deaktivieren können“. Brink bewertet die eigene Situation „durchaus selbstkritisch“, sieht sich aber in der gleichen Situation wie viele andere Behörden: „Derzeit setzen viele in der öffentlichen Verwaltung eingesetzte Anwendungen Windows voraus. Hier umzusteuern fällt vielen Verwaltungen – wie auch Privatunternehmen – natürlich schwer.“ Viele hätten sich damit in „eine faktische Abhängigkeit zu bestimmten Anbietern manövriert“, was auch eine „gefühlte Abhängigkeit“ sei. Die Handlungsspielräume seien jedoch „tatsächlich äußerst gering, gerade wenn es um stabile und sichere Kommunikation in Behördennetzen geht“. Deshalb müssten Alternativen stärker beachtet und unterstützt werden, was auch die Ausbildung betreffe (Schulzki-Haddouti, Landes-Datenschutzaufsicht: Microsoft muss Datenübertragung in Windows 10 abschalten, www.heise.de 23.03.2018; siehe auch den BBA 2018 für Windows 10, S. 95).

Bayern

BND-Funkanlage in Münchner Frauenkirche wird abgebaut

Im Nordturm der Frauenkirche in München hatte der für die Auslandsaufklärung zuständige Bundesnachrichtendienst (BND) einen „Repeater“ verbaut. Am 23.03.2018 teilte der BND mit, er werde seine Technik noch vor Ostern aus dem Liebfrauendom entfernen. Das habe man den zuständigen Stellen im Erzbistum München und Freising angeboten. Der im 98,57 Meter hohen Turm verbaute Repeater, eine Anlage zur Verstärkung von Funksignalen, sei schon seit 2011 nicht mehr genutzt worden. Laut Erzbischöflichem Ordinariat traf sich der Hausherr der Frauenkirche, Domdekan Lorenz Wolf, an diesem Tag mit einem BND-Vertreter. Wolf sprach im Anschluss von einem „einvernehmlichen Gespräch“, in dem der BND zugesichert habe, die umstrittene Anlage abzubauen. Nachdem die Technik eine Woche zuvor bekannt geworden war, hatte Wolf erklärt: „Abhörtechnik würden wir im Domturm nicht dulden“. Laut BND diente die Anlage aber allein der internen Kommunikation: Sie habe die Reichweite von vom BND genutzten Funkstrecken erhöht. „Zu keiner Zeit war die Anlage geeignet, fremde Funkverkehre abzuhören“. Laut Ordinariat ist weiterhin unklar, wann die Anlage installiert wurde; dies müsse vor 1989 geschehen sein. Klar sei aber, dass der BND dafür kein Geld an die Kirche gezahlt habe. Das einzige, was erkannt wurde, ist, dass Mitarbeiter des Geheimdienstes regelmäßig zur Wartung vorbeischauten (Wetzel, Wie kam die BND-Funkanlage in den Dom?, Stroh/Wetzel, BND baut Funkanlage in Frauenkirche ab, SZ 24./25.03.2018, 8, 46).

Saarland

Fristlose Kündigung wegen fremdnützigem Datenschutzverstoß?

Am 09.03.2018 fand ein Arbeitsgerichtstermin in Saarbrücken statt, bei dem es um die fristlose Kündigung einer Altenpflege-Expertin ging. Diese hatte bis 2017 die Fachschule bei den Saarländischen Heilstätten (SHG) geleitet. Gekündigt wurde ihr, weil sie zusammen mit einer Kollegin einen von der Geschäftsführung offenkundig hoch geschätzten Lehrbeauftragten als Hochstapler entlarvt hatte. Die SHG rechtfertigt dies mit dem Argument, dass sie gegen Datenschutzregeln verstoßen und kein Recht gehabt habe, ohne Wissen und Einwilligung der Geschäftsführung einen Kollegen zu überprüfen. Ihr Anwalt Klaus-Eckhard Walker hält dagegen, seine Mandantin habe die SHG schützen wollen.

Andere Arbeitgeber hätten sich womöglich bei Frau B. bedankt. Die SHG hingegen will sie loswerden, auch zum Leidwesen etlicher ihrer KollegInnen. Gut ein Dutzend von ihnen waren zu der Verhandlung gekommen. Sie alle kannten den Mann, Edgar S., der beste politische Verbindungen im Saarland hatte. Er saß im SPD-Landesvorstand und zählte CDU-Politiker zu seinen Freunden, darunter ganz offensichtlich auch Mitglieder der SHG-Chefetage. Fachlich war Edgar S. wenig sattelfest. Es kursierten viele Gerüchte im Haus. Frau B., die als Schulleiterin Zugang zu einer Mappe mit Qualifikationsnachweisen der Dozenten hatte, überprüfte zusammen mit einer Mitarbeiterin, ob die Zeugnisse des Mannes echt sein könnten. Sie waren es allesamt nicht. Der Ex-Dozent hatte gelogen und seine Zeugnisse bis hin zu einer Lehrgenehmigung der ka-

tholischen Kirche allesamt gefälscht. Edgar S. musste die SHG verlassen, er wurde auch angezeigt. Das Verfahren wegen Urkundenfälschung und Titelmissbrauch wurde gegen eine Zahlung von 5.000 Euro Strafe mittlerweile eingestellt.

Es stellt sich die Frage, weshalb die SHG sich von Frau B. und auch von ihrer Mitarbeiterin unbedingt trennen möchte. Eine gütliche Einigung kam 2017 nicht zustande. Schon damals hatte das Gericht erhebliche Zweifel an der Rechtmäßigkeit einer fristlosen Kündigung geäußert. Richter Arne Misol bestätigte beim Verhandlungstermin diese Bewertung: „Ich habe erhebliche Bedenken, ob das Prinzip der Verhältnismäßigkeit gewahrt wurde.“ Die SHG-Führung hätte mildere Mittel gehabt, um einen datenschutzrechtlich fragwürdigen Umgang der beiden Frauen mit Kollegen-Dokumenten zu maßregeln: ein strenges Gespräch, vielleicht eine Abmahnung. Damit hätte Frau B. leben können. Eine Kündigung aber will sie nicht hinnehmen, eine fristlose schon gar nicht. Für ein Urteil fordert Richter Misol von der SHG noch weitere Unterlagen an.

Nach den klaren Worten des Vorsitzenden zum Aspekt der Verhältnismäßigkeit lenkten die Heilstätten, ein großer und renommierter Betrieb im Saarland, nun zumindest ein wenig ein. Man sei mittlerweile bereit, eine gütliche Einigung zu suchen. Die Klägerin will aber auch keine ordentliche Kündigung akzeptieren, sie möchte zumindest einen Auflösungsvertrag und einen Ausgleich für das entgangene Gehalt und ihre Anwaltskosten. Ihr Wunsch, die ganze Angelegenheit alsbald zu den Akten zu legen, bleibt so vorerst unerfüllt.

Warum sich ihre früheren Chefs, von denen sie vor den leidigen Vorkommnissen noch 2017 ein exzellentes Zwischenzeugnis erhalten hatte, auf einmal so sehr gegen sie stellten, kann sie sich, wie sie sagt, bis heute nicht erklären. Andere hingegen können das schon: Die beiden Frauen hätten mit der Enttarnung des Hochstaplers die SHG-Führung blamiert und dortige fragwürdige Amigo-Strukturen offengelegt, mutmaßen KollegInnen aus den Heilstätten, die allesamt unter der Affäre leiden. Der Arbeitsgerichtstermin der Mitarbeiterin von Elke B., der ebenfalls fristlos gekündigt wurde, steht noch an (Höll, Zum Dank die Kündigung, SZ 10./11.03.2018, 10).

Sachsen

Im Polizeirecht auf bayerischem Kurs

Wie in vielen anderen Bundesländern (dazu Schwerpunkt DANA 1/2018) hat auch die sächsische Regierung eine Reform des Polizeigesetzes auf den Weg gebracht, wonach die Videoüberwachung deutlich verschärft und zur Straftatenverhütung ein ganzes Bündel neuer und erweiterter Befugnisse geschaffen werden soll. Ähnlich zu Bayern soll auch im benachbarten sächsischen „Freistaat“ die Polizeiarbeit weiter ins Vorfeld verlagert werden. Um Straftaten zu vereiteln, plant das dortige Innenministerium „ein ganzes Bündel neuer oder erweiterter“ Kompetenzen für die Ermittler. April 2018 wurde die Gesetzesreform auf den Weg gebracht, um das Polizeirecht umfassend zu modernisieren und an „aktuelle Erfordernisse für mehr Sicherheit“ anzupassen. So soll der Polizei „präventive Telekommunikationsüberwachung“ erlaubt werden.

Generell geht es der schwarz-roten Regierung in Dresden nach eigenen Angaben um bessere „Maßnahmen zur Abwehr terroristischer Gefahren sowie zur Bekämpfung organisierter und auch grenzüberschreitender Kriminalität“. Dazu gehörten „breitere Observationsmöglichkeiten, neue Durchsuchungsbefugnisse sowie strafbewehrte Aufenthaltsanordnungen und Kontaktverbote“. Die Videoüberwachung soll deutlich verschärft werden, vor allem „auf Verkehrsrouten, die der grenzüberschreitenden Kriminalität zur Verschiebung von Diebesgut oder als Tatorte des Menschenhandels dienen“.

Die Polizei soll künftig innerhalb eines 30-Kilometer-Korridors entlang der Grenzen zu Polen und Tschechien versuchen, Schwerverbrecher anhand der Videoaufnahmen mithilfe von Software zur automatisierten biometrischen Gesichtserkennung ausfindig zu machen. Um schwerste Straftaten zu verhindern, soll die Polizei Handy-Verbindungen unterbrechen dürfen. Für eine bessere Terrorabwehr will die Regierung die Polizei stärker bewaffnen. Spezialeinheiten sollen, so Innenminister Roland Wöller (CDU), in besonderen Einsatzsituationen über Waffen „mit erforderlicher Reichweite und hoher Durchschlagskraft wie etwa Maschinengewehre oder Handgranaten“ verfügen.

Keine Einigung besteht in der großen Koalition bei der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und bei heimlichen Online-Durchsuchungen. Die CDU befürwortet demnach den Einsatz von Staatstrojanern, um verschlüsselte Messenger-Kommunikation etwa über WhatsApp abhören und IT-Geräte ausforschen zu können. Die SPD sei jedoch dagegen, obwohl sie auf Bundesebene der Polizei bereits 2017 solche Kompetenzen selbst zur Verfolgung von Alltagskriminalität erlaubte. Umstritten ist auch noch, ob PolizistInnen in Sachsen mit Bodycams ausgerüstet werden.

Das Gesetzespaket muss den sächsischen Landtag passieren. Die Opposition hat bereits Widerstand angekündigt. Der Innenexperte der Linken, Enrico Stange, beklagte, dass unter dem Vorwand der Terrorismusbekämpfung „tiefe Eingriffe in die Grundrechte deutlich erleichtert und die sächsische Polizei weiter militarisiert“ würden. Einen „Frontalangriff auf die Bürgerrechte“ sah sein grüner Kollege Valentin Lippmann in der Initiative (Krempl, Sachsen: Polizei soll mit Gesichtserkennung und präventiver Überwachung Verbrecher jagen, www.heise.de 21.04.2018).

Sachsen-Anhalt

Leopold als Datenschutzbeauftragter nicht gewählt

Seit 2005 ist Harald von Bose Landesbeauftragter für Datenschutz in Sachsen-Anhalt. Bei der Wahl zu seiner Nachfolge fiel der von der Landesregierung vorgeschlagene Nils Leopold am 08.03.2018 im Landtag in zwei Wahlgängen und am 24.05.2018 ein drittes Mal durch. Der Vorschlag von CDU, SPD und Grünen verpasste jeweils die nötige Zwei-Drittel-Mehrheit. Nach einer Unterbrechung teilte Landtagspräsidentin Gabriele Brakebusch (CDU) am ersten

Wahltag mit, die Wahl werde vertagt. Während Leopold im ersten Wahlgang auf 48 der 79 abgegebenen Stimmen kam, entfielen im zweiten Wahlgang noch 46 Stimmen auf ihn bei zwei Enthaltungen und 31 Gegenstimmen. Beim dritten Wahlgang mehr als zwei Monate später erhielt Leopold in geheimer Abstimmung erneut 48 der 83 Stimmen, 56 Stimmen hätte er gebraucht.

Nach dem ersten Wahltag vermittelte der Linken-Fraktionschef Thomas Lippmann den Eindruck, die Nicht-Wahl von Leopold sei darauf zurückzuführen, dass sich die Koalition nicht einig sei. CDU-Fraktionschef Siegfried Borgwardt echauffierte sich daraufhin gegenüber den Linken, die Situation sei beispiellos: „Die Legendenbildung ist nicht mehr erträglich". Man lasse sich als Koalition nicht zum Sündenbock machen. Der Grünen-Abgeordnete Sebastian Striegel erklärte, in Leopold stehe ein „fachlich profilierter und höchst erfahrener Kandidat" zur Wahl: „Das ist ein schlechter Tag für den Datenschutz und die Digitalisierung". Es sei problematisch, dass ein so wichtiges Amt nur kommissarisch besetzt sei. „Der Wahl standen offensichtlich keine inhaltlichen Bedenken entgegen". Gemäß der Linken-Abgeordneten Henriette Quade hatte sie als fachpolitische Sprecherin ihrer Fraktion empfohlen, Nils Leopold zu wählen. Sie habe von niemandem gehört, der das anders gesehen hätte. Am 23.05.2018 hatten dann die Fraktionschefs von CDU, SPD und Grünen sowie der Linken angekündigt, Leopold zu unterstützen.

Teile der Grünen sahen schon im ersten Wahlgang den Nachweis fehlender Regierungsfähigkeit der Koalition. Aus Kreisen der Regierungsfraktionen heißt es, Ministerpräsident Reiner Haseloff (CDU) habe Leopold eine Woche vor dem dritten Wahlgang persönlich angerufen, um ihm mitzuteilen, er sei sein Kandidat und brauche sich deshalb keine Sorgen zu machen. Die Fraktionen warfen sich nach der Wahl gegenseitig vor, den jeweils anderen ausgetrickst zu haben. Nach dem dritten Scheitern zeigten sich die Grünen schockiert über die Wahlniederlage. Fraktionschefin Cornelia Lüddemann meinte: „Das ist mehr als ein bitterer Tag für Sachsen-Anhalt. Der Ministerpräsident muss schauen, wie wir aus diesem Chaos wieder rauskommen." Einige Grüne in Sachsen-Anhalt forderten bereits den Rücktritt des Regierungschefs.

Die Landesregierung hatte Leopold Anfang März für das Amt vorgeschlagen. Im Vorfeld der Abstimmung war der 49jährige Jurist Leopold fraktionsübergreifend als Fachmann gepriesen worden. Er hat unter anderem mehrere Jahre für den grünen Bundestagsabgeordneten Konstantin von Notz gearbeitet. Von Notz gilt als Experte für Netzweltthemen und Datenschutz. Unter anderem hatte er den NSA-Ausschuss im Bundestag begleitet, der den Abhörskandal um den US-Geheimdienst aufklären sollte.

Vor seiner Arbeit bei den Grünen arbeitete Leopold als Rechtsanwalt in Berlin, war Bundesgeschäftsführer der Humanistischen Union für Bürgerrechte und leitete zwei Jahre lang das Aufsichtsreferat beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD). CDU, SPD und Grüne hatten sich aber lange nicht auf einen gemeinsamen Nachfolger einigen können. Von Bose hatte eigentlich bereits im Frühjahr 2017 abgelöst werden sollen. Gemäß der Regelung im Land darf der LfD jeweils für sechs Jahre maximal zweimal gewählt werden. Eine dritte Amtszeit ist nicht vorgesehen. Das Gesetz fordert eine Mehrheit von zwei Dritteln der abstimmenden Abgeordneten, mindestens aber der Mehrheit der Mitglieder.

Unterdessen wurde Birgit Neumann-Becker am 08.03.2018 als Landesbeauftragte zur Aufarbeitung der SED-Diktatur wiedergewählt. Für sie stimmten 59 Abgeordnete, 21 Parlamentarier waren gegen Neumann-Becker (Leopold fällt erneut durch, www.volksstimme.de 24.05.2018; Lehman, Regierungskrise in Sachsen-Anhalt „Wir brauchen jetzt erst mal eine Denkpause", www.spiegel.de 24.05.2018; Leopold als neuer Datenschützer durchgefallen, www.mdr.de 08.03.2018; Fehlende Unterstützung, Landtag bricht Wahl des Datenschützers ab, www.mz-web.de 08.03.2018; Neuer Mann für Datenschutz, Volksstimme Sachsen-Anhalt 25.01.2018, 2).

Datenschutznachrichten aus dem Ausland

EU

Jelinek Vorsitzende des Europäischen Datenschutzausschusses

Mit dem Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) am 25.05.2018 überwacht der Europäische Datenschutzausschuss (EDSA) europaweit deren Einhaltung und koordiniert die Tätigkeit der unabhängigen Aufsichtsbehörden der 28 EU-Mitgliedsstaaten. Anfang Februar 2018 wurde Andrea Jelinek zur Vorsitzenden dieses Gremiums gewählt. Jelinek hat sich gegen ihren Kollegen aus Bulgarien durchgesetzt, der einer ihrer Vertreter wird, und löst die Französin Isabelle Falque-Pierrotin ab. Das Mandat der neuen obersten EU-Datenschützerin läuft fünf Jahre, danach könnte Jelinek einmal wiedergewählt werden. Der EDSA soll sich elf Mal jährlich treffen. Er prüft die Kohärenz der Entscheidungen der Aufsichtsbehörden und kann diese gegebenenfalls auch revidieren.

Die 57-jährige Juristin steht seit 2014 an der Spitze der österreichischen Datenschutzbehörde. Jelinek ist Mutter einer erwachsenen Tochter, fährt gern Ski und hat eine Vorliebe für das Theater. Während des Studiums war sie Referentin des Fonds zur Förderung der wissenschaftlichen Forschung und ab 1991 im Generalsekretariat der Österreichischen Rektorenkonferenz. 1993 wechselte sie ins Innenministerium,

2003 wurde sie unter Innenminister Ernst Strasser erste „Stadthauptfrau" in Wien-Landstraße. 2007 wurde sie als Anwärterin für die Nachfolge des damaligen Polizeipräsidenten Peter Stiedl gehandelt (und 2017 für den Posten einer Vizepräsidentin). 2010 übernahm die streitbare Expertin für Asyl- und Fremdenrecht die Leitung der Wiener Fremdenpolizei. 2014 wechselte sie in die Datenschutzbehörde, welche die ehemalige Datenschutzkommission im Bundeskanzleramt ersetzte. Die Stelle ist für Registrierungen zuständig, entscheidet über Datentransfers ins Ausland und genehmigt Datenverwendung für wissenschaftliche Zwecke. Österreich und Deutschland waren zum Zeitpunkt der Wahl Jelineks noch die einzigen EU-Länder, welche die DSGVO gesetzlich umgesetzt hatten (Graf, Andrea Jelinek ist „Mrs. Datenschutz", www.nachrichten.at 24.02.2018).

EU

Konservative wollen vorerst keine Datenschutzsanktionen

Europaabgeordnete von CDU und CSU haben sich dafür ausgesprochen, Verstöße gegen die neue europäische Datenschutz-Grundverordnung (DSGVO) vorerst nicht mit Sanktionen zu ahnden. Grund seien die schleppenden Vorbereitungen in den Mitgliedstaaten auf die ab Mai geltenden Regeln. Die EU-Kommission teilte Ende März 2018 mit, dass mit Deutschland und Österreich bisher nur zwei der 28 Länder die nötigen Gesetze beschlossen hätten. Der rechtspolitische Sprecher der EVP-Fraktion im EU-Parlament, Axel Voss (CDU), plädierte vor diesem Hintergrund für einen vorläufigen Sanktionsverzicht: „Der Termin des Inkrafttretens (der DSGVO) sollte gehalten werden, von der sanktionsbewährten Anwendung aber vielleicht ein weiteres halbes Jahr großzügig abgesehen werden", da die gegenwärtige Situation „sehr unbefriedigend" sei.

Dies gelte vor allem, weil 26 EU-Länder ihr nationales Recht an die Neuerungen noch nicht angepasst haben. Der CDU-Politiker kann zwar nachvollziehen, dass die notwendigen Anpassungen der administrativen und geschäftlichen Abläufe nicht einfach seien und Zeit bräuchten. „Doch kann es nicht sein, dass Deutschland und Österreich für eine fristgerechte Vorbereitung Wettbewerbsnachteile gegenüber den anderen Mitgliedsstaaten erleiden." Für einen Sanktionsverzicht zeigte sich auch die CSU-Europapolitikerin Angelika Niebler, Co-Chefin der CDU/CSU-Gruppe im EU-Parlament, offen. Sie gehe davon aus, dass die Datenschutzbehörden „im Rahmen ihrer Kompetenzen berücksichtigen, dass es bei der Anwendung der neuen Regelungen eine Anlaufphase braucht". Zugleich plädierte sie dafür, die neuen Regeln notfalls noch einmal auf den Prüfstand zu stellen: „Sollte sich tatsächlich abzeichnen, dass die Anwendung der neuen Regeln zögerlich erfolgt, werden wir die Kommission zur Evaluation auffordern und erforderlichenfalls weitere Schritte vorzuschlagen." Denn: „Sinn macht die neue Datenschutzverordnung nur, wenn sie in allen Mitgliedstaaten angewendet wird."

In ein ähnliches Horn stießen deutsche Bundestagsabgeordnete eine Woche vor dem Inkrafttreten der DSGVO anlässlich eines vertraulichen Gesprächs von Mitgliedern der Fraktionsspitze mit Vertretern des Bundesinnenministeriums. Kleine Firmen und Freiberufler könnten bei Verstößen von Abmahnvereinen und -anwälten zur Kasse gebeten werden. Vizefraktionschef Ralph Brinkhaus meinte, die Regelung fördere die Demokratieverdrossenheit und spiele der AfD in die Hände. Kollege Carsten Linnemann mahnte, wenn die Bundesregierung nichts gegen die Folgen der DSGVO unternehme, brauche sie künftig nicht mehr über Bürokratieabbau zu sprechen. Die Fraktionsführung will die Regierung dazu bewegen, kurzfristig ein Eckpunktepapier zu verabschieden, das die Praktiken unseriöser Abmahnvereine untersagt. Ein Gesetz soll so schnell wie möglich auf den Weg gebracht werden, wobei das Innenministerium beauftragt wurde zu prüfen, ob die Regeln auch rückwirkend angewandt werden können. Unzuständigkeitshalber erklärte auch die Europäische Kommission, dass nach Einführung der neuen Datenschutzregeln nicht sofort mit voller Härte durchgegriffen werde. Die EU-Kommissarin Vera Jourova erklärte am 15.05.2018, Europas Datenschutzbehörden würden in den ersten ein bis zwei Jahren sicher keine „Strafmaschinen".

Der Grünen-Europaabgeordnete Jan Philipp Albrecht sah und sieht dagegen keinen Spielraum mehr für zeitliche Aufschübe, da der Anwendungszeitpunkt durch den Gesetzgeber EU-Parlament und Rat im Gesetz festgeschrieben worden sei. „Die Kommission hat darauf keinerlei Einfluss mehr. Es ist wirklich klar: Wer am 25. Mai nicht rechtskonform sein wird, muss mit Konsequenzen rechnen" (EU-Datenschutz-Grundverordnung: Rufe nach Sanktionsverzicht, www.finanznachrichten.de 14.03.2018; Aufstand in der Union, Der Spiegel Nr. 21 19.05.2018, 21; Schonfrist bei EU-Datenregeln, SZ 16.05.2018, 5).

EU

5. Geldwäsche-Richtlinie vom EU-Parlament beschlossen

Das EU-Parlament hat am 19.04.2018 mit 574 zu 13 Stimmen bei 60 Enthaltungen eine neue Richtlinie gegen Geldwäsche und Terrorismusfinanzierung beschlossen, mit der Blockchain-Währungen aus der „Anonymität" geholt werden sollen. Finanzinstitute müssen Transaktionen jahrelang aufbewahren. Mit der 5. Richtlinie zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung werden künftig auch die Betreiber von Wechselstuben für virtuelle Währungen wie Bitcoin, Ethereum oder Ripple sowie Anbieter elektronischer Geldbörsen erfasst und reguliert, so dass auch diese ihre KundInnen im Rahmen der „üblichen Sorgfaltspflichten" für Finanzhäuser kontrollieren müssen.

Umtausch-Plattformen für Kryptowährungen müssen demnach die Identität der Nutzenden sowie deren Wallet-Adressen in einer zentralen Datenbank speichern. Sie müssen es ermöglichen, dass Details über den Einsatz der Zahlungssysteme durch Selbstangaben der Nutzenden aufgezeichnet werden können. So soll die angebliche Anonymität virtueller Währungen und

das damit verbundene „Missbrauchspotenzial für kriminelle Zwecke" reduziert werden. Zahlungen mit Bitcoin und die beteiligten Transaktionspartner lassen sich prinzipiell mit etwas Aufwand nachverfolgen.

Finanzinstitute müssen generell Belege zu sämtlichen Transaktionen fünf bis maximal zehn Jahre „nach Beendigung der Geschäftsbeziehung" aufbewahren. Da vor allem Bankkonten oft jahrzehntelang geführt werden, kann sich eine im Einzelfall nicht vorhersehbare Archivfrist ergeben. Im Idealfall sollen alle betroffenen Einrichtungen zudem ihre KundInnen identifizieren und die Daten genausolang vorhalten wie die Transaktionsbelege.

Die Verpflichteten müssen künftig ihre gesammelten Nutzerinformationen über eine zentrale Analysestelle in Form der „Financial Intelligence Unit" (FIU) zum Abruf bereitstellen. Der Anwendungsbereich der Richtlinie bleibt dabei recht vage. Alle Straftaten, die mit einer Höchststrafe von über einem Jahr belegt sind, können als Vortaten zur Geldwäsche eingestuft werden, so dass selbst einfache Delikte wie üble Nachrede grundsätzlich erfasst werden.

Anonyme Zahlungen über Prepaid-Karten werden eingeschränkt. Der bisherige europäische Schwellenbetrag von 250 Euro, für den keine Identitätsangabe nötig war, wird auf 150 Euro gesenkt. In Deutschland gilt schon ein Limit von 100 Euro. Auch bei Guthabenkarten sollen künftig strengere Auflagen zur Überprüfung von KundInnen gelten. Das EU-Parlament hat zudem jüngst dafür plädiert, dass nur noch Geld von „identifizierbaren persönlichen" Konten auf Debit-Karten eingezahlt werden können.

Die Rechtswissenschaftlerin Carolin Kaiser hatte den im Dezember 2017 zwischen Abgeordneten und Regierungsvertretern der Mitgliedsstaaten ausgehandelten Kompromiss scharf kritisiert, da damit eine unverhältnismäßige Vorratsdatenspeicherung einhergehe, umfangreiche Persönlichkeitsprofile erstellt werden können und so die Privatsphäre „praktisch wegfällt". Der Zahlungsverkehr drohe „fast vollständig überwacht" zu werden. Der EU-Datenschutzbeauftragte Giovanni Buttarelli hatte im Gesetzgebungsverfahren ebenfalls Einwände erhoben, da das Zweckbindungsprinzip nicht hinreichend beachtet werde.

Die 5. Geldwäsche-Richtlinie tritt drei Tage nach ihrer Veröffentlichung im EU-Amtsblatt in Kraft. Die Mitgliedstaaten haben dann 18 Monate Zeit, um die neuen Vorschriften in nationales Recht umzusetzen. Nur für einige der Bestimmungen gelten längere Übergangsfristen (Krempl, Geldwäsche: EU-Parlament beschließt schärfere Regeln für Kryptowährungen und Vorratsspeicherung von Finanzdaten, www.heise.de 19.04.2018).

EU

Zweiter Versuch von Facebook mit Gesichtserkennung

Rund fünf Jahre nach dem ersten gescheiterten Versuch versucht Facebook erneut, seine Gesichtserkennung in Europa wieder einzuführen. Die Nutzenden sollen selbst entscheiden können, ob sie die Funktion aktivieren oder nicht. Die Funktion war bisher aus Datenschutzgründen in Ländern der EU nicht verfügbar.

In einem Blogbeitrag teilte das Unternehmen am 28.02.2018 mit, dass zunächst einige Nutzende in Europa ausgewählt werden, um die Gesichtserkennung zu testen: „Wir fragen zunächst nur einen kleinen Prozentsatz von Menschen, damit wir sicher gehen können, dass alles ordentlich funktioniert." Mit der Funktion sollen sich künftig Betrugsversuche besser erkennen lassen. So würden Nutzende benachrichtigt, wenn ein Betrüger ein fremdes Foto als sein Profilfoto benutzt. Die Nutzenden werden auch von Facebook darauf hingewiesen, wenn sie unmarkiert auf einem Foto auftauchen, mit dessen Veröffentlichung sie vielleicht gar nicht einverstanden sind: „Sie können wählen, ob Sie sich selbst taggen, sich unmarkiert lassen oder sich an die Person wenden, die das Foto gepostet hat, wenn Sie Bedenken haben."

Von der Gesichtserkennung sollen auch Menschen mit Sehbehinderung profitieren. Ein Algorithmus verknüpft Namen mit den Personen, die auf dem Foto abgebildet sind, und liest dem Nutzenden bei Bedarf vor, wer auf dem Foto zu sehen ist. Die Einführung der von Datenschützern kritisierten Funktion erfolgt im Zusammenhang mit dem Wirksamwerden der EU-Datenschutz-Grundverordnung. In der Ankündigung verspricht Facebook den Nutzenden mehr Kontrolle über Privatsphäre-Einstellungen. Die Aktivierung sei freiwillig, werde den Nutzenden vorgeschlagen und müsse aktiv eingeschaltet werden. Wenn diese nichts unternehmen oder den Vorschlag ablehnen, bleibe die Gesichtserkennung ausgeschaltet.

Die Opt-In-Funktion war auch die Voraussetzung der Gesichtserkennungs-Gegner, die den ersten Vorstoß in Europa verhindert hatten. Im Jahr 2012/2013 scheiterte das soziale Netzwerk mit dem Versuch, die Gesichter der Mitglieder zu scannen. Datenschützer kritisierten damals die Tests und zwangen Facebook dazu, das Angebot für Europa nicht anzubieten (vgl. DANA 2014, 82). Anderenfalls würde ein neues Verfahren eingeleitet. Der US-Konzern sichert nun zu, in Zukunft datenschutzrechtliche Vorgaben zu erfüllen.

Die Gesichtserkennung ist nur eine Funktion, die getestet werden soll. In einem zweiten Test werden Facebook-Anwendende gefragt, ob sie Informationen aus dem persönlichen Profil zu persönlichen Interessen sowie politischen und religiösen Orientierungen tatsächlich mit der Öffentlichkeit teilen wollen. Facebook fragt auch diejenigen, die bislang auf solche Angaben verzichtet haben, ob sie diese nicht ausfüllen wollen (Facebook testet Gesichtserkennung in Europa, www.spiegel.de 01.03.2018; Facebook testet Gesichtserkennung auch in Europa, www.heise.de 01.03.2018).

Schengen

Mehr verdeckte Fahndungen

Die Zahl der europaweiten Fahndungen ist in den vergangenen zwei Jahren um fast die Hälfte gestiegen. Am 01.01.2018 verzeichnete das Schengener Informationssystem (SIS) mehr als 129.000 zur „verdeckten oder gezielten Kontrolle" ausgeschriebene Personen

gegenüber gut 89.000 Personen zum 01.10.2016. Das SIS basiert auf den Daten von knapp 30 Polizeidatenbanken in Europa. Jedes Land kann Personen zur verdeckten Fahndung ausschreiben. Werden diese in einem Land registriert, so wird die ausschreibende Behörde informiert, ohne dass der Betroffene unterrichtet werden muss. Andrej Hunko, auf dessen Anfrage die Bundesregierung die Zahlen mitteilte, kommentierte: „Mit dem Phänomen des islamistischen Terrorismus sind die gestiegenen Ausschreibungen nicht zu erklären. Europol meldet eine vierstellige Zahl ausländischer Kämpfer; die in 2017 hinzugekommenen Ausschreibungen betragen aber in etwa das Achtfache." Es müsse geklärt werden, warum immer mehr Menschen heimlich verfolgt werden (Der Spiegel 9/2018, 13).

UN

Vorschlag für internationale Datenzugriffsbehörde

Der UN-Beauftragte für Datenschutz bringt eine „Internationale Datenzugriffsbehörde" mit unabhängigen Richtern ins Spiel, die über grenzüberschreitende Anfragen von Sicherheitsbehörden entscheiden soll. Während der Supreme Court der USA über der Frage brütete, ob Microsoft verpflichtet werden kann, der US-Regierung Daten aus anderen Staaten auszuliefern, und die EU-Kommission an Normen zur grenzüberschreitenden „digitalen Beweissicherung" arbeitet, liegt nun auf der Ebene der Vereinten Nationen (United Nations – UN) ein Kompromisspapier auf dem Tisch, in dem der UN-Sonderbeauftragte für Datenschutz Joseph Cannataci einen „kosteneffektiven und privatsphärenfreundlichen Mechanismus" vorschlägt, über den Staaten zur Verfolgung schwerer Straftaten einschließlich Terrorismus Zugang zu persönlichen Daten in fremden Territorien erlangen könnten.

Kern der Initiative des maltesischen Rechtsprofessors ist eine „Internationale Datenzugriffsbehörde", die über grenzüberschreitende Anfragen von Sicherheitsbehörden aus den beteiligten Staaten entscheiden und gegebenenfalls einen entsprechenden Beschluss in Form eines „International Data Access Warrant" (IDAW) ausstellen soll. Wesentliche Komponente der Einrichtung ist laut dem Papier eine gerichtsähnliche Kammer mit drei bis fünf unabhängigen Richtern, die von den Vertragsparteien entsandt werden. Ihr zur Seite stehen soll ein Internationales Komitee von Menschenrechtsverteidigern, wie es der US-Kongress ähnlich bei dem geheim tagenden Überwachungsgericht FISC eingeführt hat.

Eine Berufungsinstanz in Form eines speziellen Tribunals ist ebenfalls vorgesehen. Ziel ist es, ein angemessenes Rahmenwerk für grenzüberschreitende Datenzugriffe zu etablieren, das der Rechtsstaatlichkeit verpflichtet ist und mit internationalen Menschenrechtsprinzipien im Einklang steht. Die nationale Souveränität und Rechtsprechung soll damit nicht unterlaufen, aber quasi in das internationale Rechtsinstitut ausgelagert werden, um sowohl zeitnah den praktischen Anforderungen von Ermittlern und Geheimdiensten wie der Rechtssicherheit zu genügen.

Das Richterpanel werde online über abgesicherte Videokonferenzen sehr schnell und theoretisch rund um die Uhr über einen Antrag entscheiden können, heißt es in dem Mitte Februar 2018 bei einer Expertenkonferenz auf Malta behandelten Vorschlag. Die Kammer werde ähnlich arbeiten wie erfolgreich tätige Streitbeilegungsgremien im Rahmen etwa der Weltorganisation für geistiges Eigentum (WIPO) und in Fragen von Top Level Domains (TLDs). Das Verfahren soll Anfragen über bestehende gegenseitige Rechtshilfeabkommen ergänzen, die sich oft über Monate oder gar Jahre hinziehen.

Der internationale Zugriffsbeschluss erleichtere es auch Unternehmen, mit Ersuchen nach Daten von ausländischen Sicherheitsbehörden umzugehen, wirbt Cannataci für das Konzept. Legten diese einen IDAW vor, könnten die Firmen davon ausgehen, dass mit einer solchen Durchsuchungsanordnung die Grundrechte der Betroffenen ausreichend geschützt würden und auch das Recht des Staates beachtet werde, in dem das Rechenzentrum stehe.

Insgesamt will der Sonderbeauftragte mit dem Vorhaben die staatliche Überwachung einhegen. Einschlägige bestehende und neue technische Systeme müssten eine „Menschenrechtsfolgenabschätzung" durchlaufen, automatisierte Scoring-Entscheidungen wie etwa bei No-Fly-Listen dürfte es nicht mehr geben. Staaten soll es zudem untersagt werden, Dienste- oder Hardwareanbieter dazu zu verdonnern, Sicherheitstechniken wie Verschlüsselung zu schwächen.

Die EU-Kommission plant derweil eine eigene Gesetzesinitiative, mit der Strafverfolger „elektronische Beweismittel" von Providern besser und länger sichern können sollen. Die Rede ist vor allem von Bestandsdaten wie Name und Anschrift oder möglicherweise Zugangskennungen und Passwörtern, aber voraussichtlich geht es allgemein um den Zugriff auf Daten in der Cloud. Der EU-Rat hatte die Brüsseler Regierungsinstitution im Juni 2016 aufgefordert, ein solches Instrument auf den Weg zu bringen.

Gemäß Presseberichten neigt die Kommission dazu, auf einen Kurs ähnlich dem der US-Regierung umzusteuern. Die Rede ist von einer Pflicht für Online-Anbieter mit einer Niederlassung in der EU, Daten ihrer Nutzenden auch dann auf Grundlage eines Gerichtsbeschlusses herausgeben zu müssen, wenn diese in Drittstaaten gespeichert sind. Bisher sollte es nur darum gehen, Ermittlern den Zugang zu Informationen zu erleichtern, die in anderen EU-Ländern liegen. Vera Jourová habe sich inzwischen aber der Ansicht von Strafverfolgern angeschlossen, dass die gängigen Mechanismen über Rechtshilfeabkommen „sehr langsam und ineffizient" seien. Aus Brüsseler Kreisen war zu erfahren, dass sich die Generaldirektionen für Inneres und Justiz der Kommission noch über die Ausrichtung des Gesetzesvorschlags streiten. Ausgemacht sei noch nichts, ein Entwurf liege noch nicht auf dem Tisch.

Im Microsoft-Fall hatte sich die EU-Kommission zögerlich auf die Seite des Software-Riesen geschlagen. EU-Parlamentarier kamen dagegen fraktionsübergreifend zum Schluss, dass mit der Anerkennung des US-Durchsuchungsbefehls eine ganze Reihe internationaler Vereinbarungen über den Haufen geworfen und ein Verstoß gegen die Grundrechte der EU-Bürger

gutgeheißen würde. US-DatenschutzaktivistInnen warnen vor einem globalen „Freifahrtschein" für alle nationalen Gerichtsbarkeiten. Sollte der Oberste Gerichtshof die Ansicht des US-Justizministeriums teilen, könnte jedes auch noch so autoritäre Land mit einem nationalen Beschluss „überall auf der Welt gespeicherte Daten abfragen" (Krempl, Strafverfolgung in der Cloud: UN wollen grundrechtssichere Lösung zum internationalen Datenzugriff, www.heise.de 01.03.2018).

Interpol

Verbesserter Rechtsschutz für politisch Verfolgte

Autoritäre Regime missbrauchen das weltweite Fahndungssystem Interpols, das seinen Sitz in Lyon/Frankreich hat, um politischer DissidentInnen auch im Ausland habhaft zu werden. Dies wird von Bürgerrechtsorganisationen seit Langem angeprangert. Bisher hat sich die internationale Polizeiorganisation stets gegen diesen Vorwurf verwahrt. Missbrauch sei die Ausnahme. Spätestens seit im Sommer 2017 der deutsch-türkische Schriftsteller Doğan Akhanlı aufgrund eines Interpol-Fahndungsaufrufs der Türkei im Spanienurlaub festgenommen wurde, stehen zumindest die deutschen Behörden vielem, was von Interpol kommt, deutlich kritischer gegenüber. Interpol-Fahndungsersuche, die die Türkei oder Aserbaidschan verschicken, werden in Deutschland einer vertieften Prüfung unterzogen. Nun scheint sich auch bei Interpol selbst etwas zu bewegen. Jürgen Stock, Generalsekretär von Interpol und ein ehemaliger Vizepräsident des deutschen Bundeskriminalamtes (BKA), hatte bei seinem Amtsantritt 2014 Reformen angekündigt. Im November 2016 wurde beschlossen, den Betroffenen erstmals wirksame Rechtsmittel einzuräumen, wie etwa das Recht auf Akteneinsicht, ebenso wie die Vorgabe, bestimmte Fristen einzuhalten. Die dafür zuständige Datenschutzkommission von Interpol habe seitdem auch deutlich mehr Angestellte, so eine Sprecherin der Organisation.

Ein Beispiel für die Interpol-Verfolgung von Dissidenten ist Dolkun Isa. Zwei Tage lang saß dieser 2009 im Transitbereich des Flughafens Seoul fest. Die südkoreanischen Behörden wollten Isa nach China deportieren, wo ihm eine lange Haft oder gar die Todesstrafe drohte. Verhindert wurde dies – wohl nur knapp – durch die deutschen Diplomaten, die Isa letztlich in einen Flug zurück nach München setzten. Mehr als 20 Jahre lang wurde Dolkun Isa per Red Notice von China über Interpol gesucht. Der Aktivist und heutige Präsident des „Weltkongresses der Uiguren" war Mitte der Neunzigerjahre aus China geflohen; er setzt sich seit Jahren für die Gleichberechtigung des muslimischen Turkvolks ein. In Deutschland wurde er als politischer Flüchtling anerkannt, ist seit 2006 deutscher Staatsbürger und wohnt mit seiner Familie in München. Die Festnahme am Flughafen Seoul war nicht seine einzige. 2005 wurde er in Genf und zuletzt im Sommer 2017 in Italien kurzzeitig verhaftet. In die USA und in die Türkei wurde ihm die Einreise verweigert, von Indien ein bereits ausgestelltes Visum wieder entzogen. Isa sei ein Terrorist, sagte der Sprecher des chinesischen Außenministers im Juli 2017, die internationale Gemeinschaft müsse eng zusammenarbeiten, um ihn seiner gerechten Strafe zuzuführen. Seit Herbst 2016 ist Meng Hongwei, Chinas Vizeminister für öffentliche Sicherheit, neuer Präsident von Interpol. „Chinas Arm", sagt Dolkun Isa, „ist immer länger geworden".

Ende Februar 2018 erhielt Dolkun Isa nun Nachricht aus Lyon. Interpol habe entschieden, dass seine Verfolgung durch China eine „überwiegend politische Dimension" habe. China verstoße damit gegen die Regeln der Polizeiorganisation, die in Fällen politischer Verfolgung nicht tätig werden darf. Isa ist überrascht; nach der Ernennung von Meng Hongwei zum Präsidenten habe er erst recht nicht mehr mit einer positiven Entscheidung gerechnet. Dass es mehr als 20 Jahre dauerte, bis Isas Eintrag gelöscht wurde, hat mit unzureichenden Beschwerdemechanismen bei Interpol zu tun und mit der bisher fehlenden Einsicht, überhaupt ein Problem zu haben. Mehrmals hatte Dolkun Isa Anträge auf Akteneinsicht bei der Datenschutzkommission gestellt, sie wurden ihm verweigert. Einmal musste Isa 24 Monate auf eine Antwort von Interpol warten. Dann hatte China Inhalte des Fahndungsgesuchs sperren lassen. Gegen Vorwürfe, die man nicht kennt, kann man sich nicht verteidigen.

Die Londoner Menschenrechtsorganisation „Fair Trials", die außer Dolkun Isa viele unschuldig über Interpol Verfolgte betreut, sieht die Löschung seiner Fahndung als Zeichen, dass diese Reformen bei Interpol nun greifen. Isa ist nicht der einzige Klient, der eine positive Nachricht erhalten hat, sagt der Geschäftsführer Jago Russels. Interpol habe damit begonnen, Altfälle aufzuarbeiten, bestätigen auch Justizkreise. Dass Unschuldige wie Dolkun Isa oder Doğan Akhanlı überhaupt auf die Most-Wanted-Liste geraten, vermag Interpol weiterhin nicht zu verhindern (Kampf, Eintrag gelöscht – nach 20 Jahren, SZ 13.03.2018, 6).

Österreich

Kurzfristig wurde DSGVO-Umsetzung sehr weitgehend verwässert

Kurz vor der direkten Anwendbarkeit der europäischen Datenschutzgrundverordnung (DSGVO), am 20.04.2018 beschloss der Nationalrat Österreichs und am 26.04.2018 der Bundesrat mit der Mehrheit der Regierungsparteien ÖVP und FPÖ erneut Änderungen des Datenschutzrechts, um der DSGVO den neuen Biss und die Wirksamkeit zu nehmen. Die meisten Verstöße werden darüber für straffrei erklärt; Datenschutz-NGOs wird die Möglichkeit verweigert, Schadenersatzansprüche zu stellen. Neben dem Datenschutzgesetz (DSG) wurden noch mehr als 140 weitere Gesetze überarbeitet.

Seit dem 25.05.2018 gilt die DSGVO, die drakonische Sanktionen bei Datenschutzverstößen vorsieht, auch in Österreich. Doch dort soll es Strafen in aller Regel nur für Wiederholungstäter geben; selbst davon gibt es Ausnahmen. Öffentliche Einrichtungen sollen immer straffrei davonkommen. Für Spione – auch von ausländischen Nachrichtendiensten – ist eine Generalausnahme vorgesehen. Hinzu kommen Erleichterungen für Videoüberwachung und

deren Auswertung. Und wer vor dem 25.05.2018 den Datenschutz verletzte, wird nach der alten oder neuen Rechtslage (nicht) bestraft, je nachdem, was für den Täter günstiger ist. Die Regelung, dass gemeinnützige Organisationen, die im Auftrag betroffener Bürger Datenschutzverletzungen zur Anzeige bringen, von den Tätern keinen Schadenersatz verlangen dürfen, trifft beispielsweise die Initiative noyb (none of your business) von Max Schrems, der durch mehrere Verfahren gegen Facebook bekannt geworden ist und mit dieser NGO Sammelklagen durchführen möchte.

Völlig neu ist ein Journalisten-Privileg, wonach Medien personenbezogene Daten für journalistische Zwecke verarbeiten und dabei die Kapitel II, III, IV, V, VI, VII und IX der DSGVO ignorieren dürfen. Die Datenschutzbehörde muss das Redaktionsgeheimnis berücksichtigen. Für wissenschaftliche, künstlerische und literarische Zwecke gilt ein schwammig gefasstes Privileg bei der Verarbeitung personenbezogener Daten. Ausgewählte Teile der DSGVO finden dabei keine Anwendung, „soweit dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen".

Bereits 2017 war ein weitgehend gelockertes Sonder-Datenschutzregime für Strafverfolger und Strafvollzug beschlossen worden. Die jüngste Novelle erweitert diese Privilegien auf Spionage und „militärische Eigensicherung". Diese sollen offenbar für Spione aller Staaten gelten; eine Einschränkung auf österreichische Nachrichtendienste gibt es nicht. Sogar private Spionagedienste kommen in den Genuss der weitgehend gelockerten Datenschutzauflagen, wenn sie im Auftrag eines EU-Mitgliedsstaates spionieren. Wenn die Polizei die für sie geltenden relativ lockereren Bestimmungen verletzt, muss sie keine wirksamen Strafen fürchten. In § 30 Abs. 5 des DSGVO-Umsetzungsgesetzes heißt es: „Gegen Behörden und öffentliche Stellen, die insbesondere in Formen des öffentlichen Rechts, sowie des Privatrechts eingerichtete Stellen, die im gesetzlichen Auftrag handeln, und gegen Körperschaften des öffentlichen Rechts können keine Geldbußen verhängt werden."

Für private Datenverarbeiter werden in § 11 der DSGVO die Zähne gezogen, um die „Verhältnismäßigkeit" des Strafenkatalogs der DSGVO (Art. 83) zu sichern: „Insbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen." Es soll das Grundprinzip „Verwarnen statt Strafen" gelten. Nur besonders hartnäckige Täter, die keine Behörde sind, sollen belangt werden können. Von der rechtskonservativen Koalition, die sonst gerne Strafverschärfungen beschließt, wurden bei der DSGVO also die Samthandschuhe ausgepackt. Gestrichen wurde ein im Vorjahr beschlossenes Privileg für Arbeitnehmervertreter. Nach Ansicht von Max Schrems sind die Regelungen europarechtswidrig, weil gemäß der DSGVO die Strafen „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sein müssen. Er nannte die Umsetzung eine „fast ungarische Dreistigkeit".

Selbst wenn Unternehmen hartnäckig den Datenschutz verletzen, müssen sie sich in Österreich nicht fürchten, da gemäß einem schon 2017 beschlossenen § 30 DSG sie für Gesetzesverletzungen untergeordneter Mitarbeiter nicht bestraft werden können. Nur wenn das Management oder eine unternehmensinterne Kontrolleinrichtung wiederholt den Datenschutz verletzt, kann die Datenschutzbehörde Strafen aussprechen. Und verhängt eine andere Verwaltungsbehörde eine Verwaltungsstrafe, kann die Datenschutzbehörde ihrerseits nicht mehr strafen – egal, wie hoch die andere Verwaltungsstrafe war. Unternehmen, deren Management zum wiederholten Male den Datenschutz missachtete, sind also gut beraten, sich nach einer anderen Bestimmung mit einer kleinen Verwaltungsstrafe sanktionieren zu lassen, um so endgültig den neuen, womöglich spürbaren Strafen der Datenschutzbehörde zu entgehen.

Schon 2017 wurde Videoüberwachung zum Objekt- und Personenschutz weitgehend legalisiert, sofern kein gelinderes Mittel zur Verfügung steht. Diese Einschränkung wurde nun gestrichen, so dass Videoüberwachung auch dann zulässig ist, wenn es datenschutzfreundlichere Sicherheitsvorkehrungen gäbe. Zugleich wurde die Liste von ausdrücklich unzulässigen Bildverarbeitungen reduziert. Es sollte als unzulässig gelten, personenbezogene Fotos oder Videos mit anderen personenbezogenen Daten abzugleichen. Dies ist nun nur noch unzulässig, wenn damit ohne Zustimmung der Betroffenen Persönlichkeitsprofile erstellt werden sollen.

Österreich hatte bereits 2017 das Datenschutzgesetz (DSG) aus dem Jahr 2000 grundlegend neu gefasst und an die DSGVO angepasst. Noch vor dem Wirksamwerden am 25.05.2018 erstellte die Regierung eine weitere Novelle, mit der auch einige Verfassungsbestimmungen geändert werden sollten. Diese Novelle wurde öffentlich konsultiert, im zuständigen Verfassungsausschuss des Nationalrats diskutiert, dort mit den Stimmen von ÖVP, FPÖ und SPÖ bestätigt, und dem Plenum des Nationalrats als wichtigere Kammer des österreichischen Bundesparlaments zur Beschlussfassung vorgelegt.

Doch dann verweigerte die SPÖ ihre Zustimmung: Sie hatte einen (als Minderheitenrecht konzipierten) Untersuchungsausschuss über zweifelhafte Vorfälle im Inlands-Nachrichtendienst BVT beantragt, was von den Regierungsparteien blockiert wurde. Da bekam die SPÖ Bedenken über die Verfassungsänderungen beim Datenschutz. Ohne ihre Zustimmung haben die Regierungsfraktionen aber nicht genügend Stimmen für Verfassungsänderungen. Daraufhin brachten Abgeordnete von ÖVP und FPÖ einen Abänderungsantrag zu ihrer Novelle ein. Dabei entfernten sie nicht einfach die Verfassungsbestimmungen, sondern schrieben die Novelle gleich in weiten Teilen um. Am Ende stimmten die Nationalratsabgeordneten der Regierungsparteien ÖVP und FPÖ dafür, die Abgeordneten von SPÖ, Neos und der Liste Pilz dagegen. Experten wurden zum neuen Text nicht mehr angehört. Max Schrems von noyb kritisierte nicht nur den Inhalt, sondern auch die Masse an verabschiedeten Gesetzen, da dadurch der Überblick verloren gehe. Die unerwarteten Änderungen traten sämtliche am 25.05.2018 in Kraft, nachdem der Bundesrat (Länderkammer), wo ÖVP und FPÖ über eine breite Mehrheit

verfügen, auch zustimmte (Sokolov, Keine Strafen: Österreich zieht neuem Datenschutz die Zähne, www.heise.de 24.04.2018; Kaiser, Österreich verwässert die EU-Datenschutzgrundverordnung, netzpolitik.org 26.04.2018).

Schweiz

DNA-Phänotypisierung soll erlaubt werden

Bisher ist es in der Schweiz erlaubt, anhand von kleinsten Abstrichen von Speichel, Sperma oder Haut eine Person zu identifizieren. Aus der DNA wird ein allgemeiner Fingerprint hergestellt und in einer zentralen Datenbank gespeichert. Einzelne Gene eines Menschen auf individuelle Merkmale hin zu analysieren ist bisher verboten. Doch ist die Diskussion über genetische Phänotypisierung nun auch in der Schweiz angekommen. Auslöser ist der Fall Emmen: Im Juli 2015 zerrte ein Mann eine junge Frau vom Fahrrad, vergewaltigte sie und ließ sie schwer verletzt zurück. Der Täter ist immer noch nicht gefasst. Die Hoffnung: Wenn die DNA Hinweise auf sein Aussehen gäbe, wäre er zu finden.

Der Luzerner FDP-Politiker Albert Vitali, der das Opfer der Straftat persönlich kennt, hat einen Vorstoß ins Parlament gebracht, der erlauben soll, bei schweren Verbrechen die DNA-Analyse auszuweiten: „Neu könnte man mit der sogenannten verschlüsselten DNA zum Beispiel die Augen- und Hautfarbe herausfinden, damit ein Robotbild erstellen und die Täterschaft viel genauer ermitteln." Noch im Jahr 2018 soll ein Gesetzesentwurf in die Vernehmlassung gehen.

Die DNA-Phänotypisierung ist ein Verfahren, mit dem Rückschlüsse aus dem Genom, also der DNA eines Individuums, auf dessen äußere Merkmale (Phänotyp) gezogen werden. Die Rechtsmedizin (Forensik) bedient sich in manchen Ländern bereits solcher Methoden zur Täterermittlung oder um Tatverdächtige auszuschließen (vgl. DANA 1-2018, 20 f.).

Das Institut für Rechtsmedizin der Universität Bern verfügt über ein Gerät der neuesten Generation zur Durchführung solcher Analysen. Mitarbeitende haben es mit gemischtem Erfolg mit ihrer eigenen DNA getestet: Silvia Utz, die Abteilungsleiterin, findet ihre eigene Auswertung gut. Demnach ergab die Vorhersage mit über 80% Wahrscheinlichkeit, dass sie blonde Haare habe. Die blauen Augen wurden sogar zu 96% vorausgesagt. Im Team gebe es aber auch Leute, die mit ihrer Vorhersage nicht ganz zufrieden sind: „Das Ganze ist heute also noch mit Vorsicht zu genießen."

Mit einer recht hohen Zuverlässigkeit vorhersagen können die heutigen Analysen auffällige Haarfarben, wie blond, rot oder schwarz und eine deutliche Augenfarbe, wie blau und braun. Jedoch bei Mischformen, wie sie im mitteleuropäischen Raum häufig vorkommen, wird die Aussage unzuverlässig, wie zum Beispiel bei bräunlichen Haaren oder grünen Augen. Über DNA-Analysen soll auch die biogeographische Herkunft einer Person bestimmt werden. An der Bestimmung anderer Eigenschaften, wie zum Beispiel des Alters einer Person, wird gearbeitet.

Silvia Utz: „Sehr interessant für eine Ermittlung wäre ja die Körpergröße eines Menschen. Diese kann man recht schlecht beeinflussen oder fälschen." Allerdings habe sich herausgestellt, dass die Körpergröße nur etwa zu 80% genetisch bedingt sei; eine Rolle spielten andere Faktoren wie zum Beispiel die Ernährung. Abgesehen von Augen- und Haarfarben seien Vorhersagen noch unsicher: „Die Erwartungen sind aktuell viel zu hoch, sie entsprechen nicht dem, was heute möglich ist."

Dennoch soll die Politik nun entscheiden, ob die DNA-Phänotypisierung der Verbrechensaufklärung dienen soll. Balthasar Glättli von den Grünen erklärte hierzu, dass noch Vorsicht angebracht ist aus zwei Gründen: Erstens, dass man übergeneralisiere und einen Generalverdacht hege, und „dass die Leute dann beweisen müssen, dass sie unschuldig sind – und nicht mehr, dass der Staat beweisen muss, dass sie schuldig sind." Dies sei ein grundlegendes Rechtsprinzip. Man mache den Opfern zudem zu viel Hoffnungen: dass ein Phantombild erstellt werden könne, mit dem sich der Täter sehr schnell finden lasse: „Das wird auch weiterhin nicht der Fall sein". Das Parlament muss jetzt entscheiden, ob und wenn ja welche Gene der DNA entschlüsselt werden dürfen und bei welchen Verbrechen (Schwerzmann, Gesetz zur DNA-Phänotypisierung ist in der Pipeline, www.srf.ch 04.04.2018).

Wales

Hohe Fehlerquote bei polizeilicher Echtzeit-Gesichtserkennung

Seit 2017 testet die Polizei in Wales ein System zur automatischen Gesichtserkennung in Echtzeit. Beim Finale der Champions League in Cardiff lag sie in 92% der Fälle falsch. Dies geht aus den Daten zu dem Pilotversuch des Systems hervor, welche die Polizei von Südwales veröffentlicht hat. Rund um das Spiel waren etwa 170.000 BesucherInnen in der Stadt und das System hat 2.470 mögliche Treffer angezeigt, von denen sich aber 2.297 als falsch herausstellten. Ein Polizeisprecher verteidigte das System und die damals erzielte Trefferrate von gut 7% und meinte, kein System sei hundertprozentig korrekt. Niemand sei infolge eines derartigen „False Positives" festgenommen worden und aus der Öffentlichkeit habe sich niemand beschwert.

Die Polizei erklärt die hohe Fehlerrate beim Finale der Champions League mit der „schlechten Qualität" der Fotos, die von Europas Fußballverband UEFA, Interpol und anderen Partnern geliefert worden seien. Bei anderen Rückgriffen auf die Technik gab es den Angaben zufolge deutlich weniger angezeigte Treffer, aber meist immer noch mehr falsche als richtige.

Schon bei Ankündigung des Tests kritisierten DatenschützerInnen, dass die rechtlichen Bestimmungen der zunehmend eingesetzten und weiterentwickelten Überwachungstechnik nicht nachkämen. Die automatische Gesichtserkennung generiere sensible Daten zu tausenden von Menschen und es sei nicht geklärt, was mit diesen geschehen werde. Angesichts der nun veröffentlichen Daten erklärte BigBrotherWatch: „Nicht nur ist die automatische Gesichtserkennung in Echtzeit eine Gefahr für Bürgerrechte, sie ist auch ein gefährlich ungenaues Polizeiwerkzeug" (Holland, Gesichtserkennung bei

Champions-League-Finale: Tausende fälschlich als Kriminelle identifiziert, www.heise.de 07.05.2018).

USA

„Golden State Killer" mit DNA-Beinahetreffer identifiziert

In Kalifornien wurde im April 2018 mit Hilfe eines Datenabgleichs über eine öffentlich zugängliche DNA-Datenbank der 72jährige Joseph James DeAngelo als Täter von mindestens 51 Vergewaltigungen und 12 Morden identifiziert, die er von 1976 bis 1986 begangen hatte. Kunden der Gentest-Firma GEDMatch, die Familienforschung als Service anbietet, laden ihre genetischen (DNA-) Daten in eine öffentlich zugängliche Datenbank hoch, um Verwandtschaftsverhältnisse zu erkunden. Diese Gendaten haben sie zuvor von größeren Anbietern wie z. B. der Google-Tochter 23andMe analysieren lassen.

Die Muttergesellschaft von Family-TreeDNA „Gene by Gene" hatte im März 2017 eine gerichtliche Anordnung des Eastern District of California erhalten mit der Anforderung von „begrenzten Informationen" zu einem einzelnen Kundenkonto. Es ging, gemäß den Angaben von Paul Holes, einem inzwischen ausgeschiedenen Ermittler der Staatsanwaltschaft des Contra Costa County District, konkret um das Auffinden des Namens des Täters über die Angaben zur Familienforschung: „Wir wollten sowohl die Identität wie auch die Kontodaten des Auftraggebers des Tests ausfindig machen".

Holes und seine Kollegen suchten nach Treffern in den Profilen der von Family-TreeDNA betriebenen öffentlichen Datenbank YSearch, in der genetische Informationen des Y-Chromosoms gespeichert sind, die vom Vater an den Sohn vererbt werden. Die Ermittler kannten aus Tatortspuren 67 genetische Marker im Y-Chromosom des Mörders. Alle drei Monate wurde gemäß der gerichtlichen Anordnung auf der Basis von 12 genetischen Markern ein Abgleich durchgeführt, bis es einen Treffer gab. Einer der Marker war für westeuropäische Abstammungen untypisch. Die Anforderung von Angaben zum Probengeber und von Zahlungsdaten erfolgte, weil Tests oft unter falschem Namen in Auftrag gegeben werden. Im konkreten Fall erfolgte die Zahlung durch eine Frau, die mit der DNA ihres Vaters Informationen zu ihrem Familienstammbaum suchte. Dieser Vater war nach Aufforderung der Ermittler bereit, seine DNA zur Verfügung zu stellen und es zeigte sich auf der Grundlage aller 67 Marker, dass er nicht der Gesuchte ist, dass es aber einen gemeinsamen männlichen Vorfahr gab. Daraufhin wurde die Tochter kontaktiert und um weitere Informationen zu ihrem Familienstammbaum gebeten.

Januar 2018 nutzten die Ermittler eine gekühlt aufbewahrte Genprobe eines 37 Jahre alten Mörders in Ventura County in Südkalifornien. Mit diesen umfassenden DNA-Daten, ergänzt um die bekannten Daten des gesuchten Täters, war es den Ermittlern möglich, ein „Microarray" durchzuführen, bei dem parallel ein Detailabgleich mit mehreren Hunderttausend Markern auf dem gesamten Genom durchgeführt werden kann. Diese Technologie wird auch von genetischen Familienforschenden angewendet, um mögliche Verwandte zu finden. Die Ermittler im Fall des Golden State Killers führten mit dem erstellten DNA-Profil unter falschen Angaben einen Abgleich bei GEDMatch durch. Will jemand eine Familienanalyse durchführen lassen, so muss der Kunde erklären, dass es sich um die eigenen Daten oder die einer Person handelt, für die er als gesetzlicher Vertreter zur Eingabe und Abfrage berechtigt ist. Bei dem GEDMatch ergab sich der Verdacht, dass das verwendete Profil zu einem Cousin zweiten Grads des Mörders passte. In der folgenden Auswertung von Datenbanken und Lokalzeitungen wurde mit Hilfe der erlangten Daten versucht, lebende Personen aus dem Familienstammbaum auszumachen, die in Verbindung standen zu den Orten, an denen sich die Morde und Vergewaltigungen ereignet hatten. Zwar erwies sich der erste Treffer als falsch. Doch wurden sie über diesen primären Verdächtigen auf dessen Bruder hingewiesen, der auch freiwillig seine DNA-Probe zur Verfügung stellte. Es dauerte weitere 4 Monate für ein Ermittlungsteam von 5 Personen, um vom Cousin dritten bzw. vierten Grads zu DeAngelo als neuem Hauptverdächtigen zu gelangen. Die Ermittler analysierten Material die DNA dieses Hauptverdächtigen und stellten nun eine vollständige genetische Übereinstimmung fest.

Nachdem dieser Ermittlungserfolg bekannt geworden war, veröffentlichte GEDMatch mit Datum vom 27.04.2018 folgenden Text: „Wir haben festgestellt, dass die GEDMatch-Datenbank zur Identifizierung des Golden State Killers genutzt wurde. Wir wurden nicht von Ermittlungsbehörden oder über sonst jemanden über den Fall oder die DNA angesprochen. Es gehört schon immer zur Politik von GEDMatch, seine Kunden darüber zu informieren, dass die Datenbank für andere Zweck genutzt werden kann. Die Datenbank dient der Familienforschung, doch sollten die Teilnehmer bei GEDMatch verstehen, dass ihre DNA für andere Zwecke einschließlich der Identifikation von Verwandten, die Verbrechen begangen haben oder Opfer von Verbrechen waren, genutzt werden kann. Sollten Sie solche Nutzungen, die mit Familienforschung nichts zu tun haben, nicht wollen, so sollten Sie Ihre DNA nicht hochladen und/oder diese, wenn sie hochgeladen ist, löschen. Wenn Sie eine Löschung durchführen wollen, kontaktieren Sie gedmatch@gmail.com."

Direkt nach der Festnahme des Verdächtigen erklärten die drei führenden Genanalysefirmen in den USA, 23andMe, Ancestry und FamilyTreeDNA, dass sie nicht in die Ermittlungen einbezogen waren. 23andMe hat mehr als 5 Mio. KundInnen, Ancestry.Com führte schon 10 Mio. Analysen durch. Gemäß einem Transparenzbericht von 23andMe vom 15.12.2017 hatte das Unternehmen in den vergangenen 11 Jahren fünf Behördenanfragen zu 6 Kunden erhalten, ohne aber diesen Anforderungen nachzukommen. Doch bestätigten die Firmen, dass sie gerichtlichen Anordnungen folgen würden.

Der konkrete Fall des Golden State Killers war nicht der erste, bei dem einer gerichtlichen Anforderung entsprochen wurde. So erhielt Ancestry im Jahr 2014 einen Gerichtsbeschluss zur genetischen Identifizierung in der Sorenson Molecular Genealogy Foundation Datenbank, die das Unternehmen kurz zuvor erworben hatte. Die gesuchten Genmarker auf dem Y-Chromosom gehörten zum Vater von Michael Usry, einem Filmpro-

duzenten in New Orleans. Die Polizei erzielte einen Beinahetreffer zu einer Samenprobe, die von der Ermordung von Angie Dodge im Jahr 1996 stammte. Dodge war in ihrer Wohnung erstochen worden. Der zunächst verdächtigte Usry wurde nach einer umfassenderen Genanalyse entlastet. Nach den Erfahrungen mit diesem Fall, so ein Sprecher von Ancestry, „haben wir dafür gesorgt, dass die Daten in der privaten Verfügungsmacht der Kunden verbleiben". Es habe sich um die einzige rechtsförmliche Anfrage gehandelt, die Ancestry bisher erhalten habe.

Die genetische Familienforscherin CeCe Moore, Gründerin von DNA Detectives, einer Gruppe, die Adoptierten hilft, ihre biologischen Eltern oder aus den Augen verlorene Verwandte zu finden, erklärte zu dem aktuellen Fall des Golden State Killers: „Ich hatte in den vergangenen Jahren schon viele schlaflose Nächte, dass dies einmal passieren würde." Bei ihr hätten schon mehrfach Ermittlungsbehörden um Hilfe beim Lösen von Mord- und Vergewaltigungsfällen angefragt. Doch habe sie dies stets verweigert, „weil ich immer noch nicht mit den ethischen Fragen klarkomme, die sich bei der Verwendung von Familienforschungsdatenbanken zum Finden von Kriminellen stellen".

Der Fall löste in den USA eine heftige Debatte unter JuristInnen, KriminalistInnen, Forschenden, Angehörigen von besonders diskriminierungsgefährdeten Minderheiten und der Öffentlichkeit aus, welche unbeabsichtigten Konsequenzen das Preisgeben von Gendaten haben kann und was in diesem Zusammenhang zulässig ist (Aldous, Cops Forced A Company To Share a Customers's Identity For The Golden State Killer Investigation, www.buzzfedd.com 01.05.2018; Kolata/Murphy, The Golden State Killer Is Tracked Trough a Thicket of DNA, and Experts Shudder, www.nytimes.com 27.04.2018).

USA

FDA erlaubt BRCA-Test ohne genetische Beratung

Die US-Gesundheitsaufsichtsbehörde, die Food and Drug Administration (FDA), hat dem Google-Ableger 23andMe den Verkauf eines Gentests erlaubt, mit dem drei Mutationen der Brustkrebsgene BRCA1 und BRCA2 festgestellt werden. Diese Varianten sind in der jüdischen Ashkenazi-Bevölkerung weit verbreitet, in einem erheblich geringeren Maß bei Menschen mit einem anderen ethnischen Hintergrund. Noch 2013 hatte die FDA 23andMe verboten, jegliche Form von genetischen Gesundheitstests für Endkunden anzubieten. 2015 erhielt das Unternehmen die FDA-Erlaubnis für die Testung ohne ärztliche Verschreibung des Bloom-Syndroms sowie 2017 für Risikoberichte zur Parkinson- und zur Alzheimer-Krankheit. Bei Frauen mit bestimmten Genvarianten besteht eine 45%- bis 85%-Wahrscheinlichkeit für eine Brustkrebserkrankung bzw. eine 44% bzgl. Eierstockkrebs. Bekannt wurde der Fall von Angelina Jolie, die nach einem positiven Test auf ein BRCA-Gen eine doppelte Mastektomie vornehmen ließ.

Anne Wojcicki, Mitgründerin und Chief Enterprise Officer von 23andMe, erklärte dazu: „Es ist ein wichtiger Meilenstein für 23andMe und für die Verbraucher, als erstes und einziges Genanalyse-Unternehmen mit direkter Endkundenbeziehung von der FDA die Erlaubnis bekommen zu haben, das Krebsrisiko ohne ärztliche Verschreibung zu untersuchen." Eric Topol vom Scripps Research Institute warnte dagegen, dass der Test nur drei Mutationen überprüft und so die Getesteten die falsche Vorstellung entwickeln können, keine gefährliche Mutation zu haben, „wobei sie möglicherweise eine andere von den hunderten Mutationen mit der gleichen Wirkung haben". Mary-Claire King von der University of Washington wies auf die täuschende Wirkung dieses Tests hin: „Wenn Frauen eine ernsthafte Mutation haben und dies nicht wissen, können diese an Brust- oder Eierstockkrebs sterben, weil sie fälsch wegen des Testergebnisses annahmen, dass alles normal wäre".

Auch die FDA bestätigt, dass ein negativer Befund nicht bedeutet, dass eine Person keine BRCA-Mutation in anderen Genen mit Erkrankungsrisiko hat, die nicht getestet wurde. Kliniker dürften auf der Grundlage dieses Tests nicht ihre Behandlung durchführen. Auch könne der Test keine ärztliche Beratung ersetzen. Auch Wojcicki meinte, dass ihr Test niemanden davon abhalten solle, an Brustkrebs-Screening-Maßnahmen teilzunehmen. 23andMe bietet direkt keine genetische Beratung an, sondern beschränkt sich auf Webseiten, auf denen die Bedeutung des Tests erklärt wird (genomeweb 07.03.2018, 23andMe´s Test OK´d; Zhang, 23andMe Will Now Test for BRCA Breast-Cancer Genes, www.theatlantic.com 06.03.2018).

USA

Protest gegen Zensus-Frage nach Staatsangehörigkeit

Alle zehn Jahre verschickt die US-Bundesregierung in Washington einen Fragebogen an die Haushalte des Landes. Damit ermittelt sie nicht nur Anzahl der EinwohnerInnen, sondern auch weitere Daten, die z. B. als Grundlage für die regelmäßige Überprüfung der Wahlkreise herangezogen werden. Auch die Zuweisung von Bundesgeldern an die Gliedstaaten stützt sich auf die Haushaltszählung.

Ende März 2018 gab das zuständige Handelsministerium bekannt, beim nächsten für das Jahr 2020 vorgesehenen Zensus eine neue Frage einzubauen: jene nach der Staatsbürgerschaft. Diese Frage ist in vielen Ländern unumstritten. Im Zensus der deutschen Bundesregierung von 2011 fand sich eine entsprechende Frage gleich zu Beginn. In den USA löste die Ankündigung dagegen Aufregung aus, weil sie die politische Landschaft nachhaltig verändern könnte. Eine Reihe von zumeist demokratisch regierten Bundesstaaten, darunter Kalifornien und New York, kündigten an, dagegen zu klagen. Sie sehen hinter der neuen Erhebungsmethode ein politisches Manöver der Regierung von Präsident Donald Trump.

Vermutet wird, dass besonders Einwanderer ohne gültige Aufenthaltspapiere den Fragebogen nicht ausfüllen werden, weil sie befürchten, dass ihre Daten an die Migrationsbehörden weitergegeben werden und dass ihnen dann die Abschiebung drohen würde. So erklärte eine Frau aus Guatemala der Presse: „Ich würde darauf niemals ant-

worten, ich habe keine gültigen Papiere". Auch legale EinwanderInnen würden sich zweimal überlegen, ihre Daten an die Regierung weiterzugeben, sagte eine Sprecherin der Organisation National Immigration Forum. Dafür seien das Misstrauen und die Angst zu groß.

Nach Schätzungen des Pew-Instituts leben in den USA rund 22 Millionen EinwanderInnen, die keine US-amerikanische Staatsbürgerschaft haben. Gut die Hälfte davon besitzt keine gültigen Aufenthaltspapiere. Sollten sich viele dieser Menschen nicht am Zensus beteiligen, würde das zu gröberen Verzerrungen in der Haushaltserhebung führen. Bundesstaaten wie Kalifornien, in denen EinwanderInnen einen großen Anteil an der Bevölkerung ausmachen, könnten dann Sitze im Kongress verlieren. Dies ginge politisch zulasten der Demokraten.

Der kalifornische Generalstaatsanwalt Xavier Becerra schrieb in seiner Klage gegen die Entscheidung, das Vorgehen der Trump-Regierung sei verfassungswidrig. Mit ihrem „willkürlichen" Akt unterlaufe die Regierung die Auflage, alle BewohnerInnen des Landes zu erfassen. Maura Healey, Generalstaatsanwältin von Massachusetts, sprach von einem „durchsichtigen und illegalen Versuch" der Regierung, den Zensus für ihre politischen Ziele zu kapern.

In der Haushaltsbefragung werden die Amerikaner regelmäßig nach ihrer ethnischen Zugehörigkeit gefragt. Die Staatsangehörigkeit wurde jedoch letztmals im Jahr 1950 erhoben. Es gehe darum, möglichst genaue Daten zu erhalten, um gegen Wahlbetrug vorgehen zu können, verteidigten Regierungsvertreter die Maßnahme. Nach einem Bericht der Recherche-Plattform Pro Publica hatten sich Beamte der Zensusbehörde gegen den Schritt gewehrt. Der Beschluss sei nach einer Intervention des Justizministeriums gefallen.

Ob die Teilnahme der EinwanderInnen am Zensus tatsächlich zurückgehen würde, ist umstritten. US-Handelsminister Wilbur Ross verwies darauf, dass die Staatsbürgerschaft in anderen Umfragen schon länger erhoben werde. Dort habe man keine geringere Beteiligung festgestellt. Diese Umfragen gehen allerdings jeweils nicht an alle EinwohnerInnen des Landes. Zudem gibt es für die Skepsis der Einwanderer historische Gründe. Während des Zweiten Weltkriegs lieferte die Zensurbehörde die Namen und Adressen von EinwohnerInnen mit japanischen Wurzeln an die Geheimdienste. Nach dem Angriff auf Pearl Harbor schickte sie die Daten von japanischstämmigen AmerikanerInnen auch noch an die Armee. Tausende von ihnen landeten in Internierungslagern (Cassidy, Empörung über Zensus-Frage, SZ 29./30.03.2018, 8).

Neuseeland

Dotcom gewinnt im Auskunftsverfahren gegen Regierung

Die Regierung Neuseelands muss Kim Dotcom umfangreiche Akten zur Verfügung stellen, die sie ihm seit 2015 rechtswidrig vorenthält. Dazu kommt eine Entschädigung. Dotcom glaubt nun, seine Auslieferung an die USA verhindern zu können. Das Menschenrechtsgericht des Landes (Human Rights Review Tribunal) entschied, dass die Regierung Neuseelands die Rechte des Klägers Dotcom verletzt hat, indem sie ihm die Herausgabe über ihn gespeicherter Daten verweigert. Die Regierung soll Dotcom nun die bereits 2015 unter Berufung auf ein Datenschutzgesetz angeforderten Unterlagen geben. Zusätzlich muss sie ihm 90.000 neuseeländische Dollar (umgerechnet rund 53.000 Euro) Entschädigung zahlen. Bereits vor längerer Zeit war festgestellt worden, dass die Regierung Dotcom illegal ausspioniert und die Überwachung gegenüber Richtern verschwiegen hatte.

Dotcom wollte die über ihn gespeicherten Informationen insbesondere für das Gerichtsverfahren nutzen, in dem er sich seit 2012 gegen US-Auslieferungsersuchen zur Wehr setzt. Der Deutsche war noch nie in den USA. Dennoch will ihm die US-Regierung dort einen Strafprozess wegen Urheberrechtsverletzung, Racketeering und Geldwäsche machen. Ebenso sollen ehemalige Geschäftspartner Dotcoms ausgeliefert werden, die sich ebenfalls wehren. Dotcom freute sich über Twitter über die am 26.03.2018 veröffentlichte Entscheidung: „Durch die rechtswidrige Unterdrückung von Informationen, die mir in [meinem Auslieferungsverfahren] helfen könnten, hat [Neuseeland] den Verlauf des Gerichtsverfahrens pervertiert". Er sieht den Anfang vom Ende des Auslieferungsverfahrens gekommen. Außerdem forderte er den neuseeländischen Datenschutzkommissar zum Rücktritt auf. Der Beamte hatte nach einer Beschwerde Dotcoms für die Regierung entschieden – gemäß dem jetzt ergangenen Urteil zu Unrecht. Zudem werde er damalige Regierungsmitglieder verklagen, die sich gegen die Ausfolgung seiner Daten ins Zeug geworfen hatten (Sokolow, Auskunft verweigert: Neuseeland muss Kim Dotcom entschädigen, www.heise.de 26.03.2018).

China

Amnesty kritisiert Cloud-Umzug auf Regierungsserver

Die Menschenrechtsorganisation Amnesty International äußerte sich besorgt über die Verlagerung von iCloud-Daten auf chinesische Server: Dies könne lokalen Behörden die Überwachung von Apple-Nutzenden ganz ohne eine Hintertür ermöglichen. Der Umzug von iCloud-Daten auf die Server einer chinesischen Firma „löst große Bedenken aus, dass Behörden Apple-Nutzer in China nun unbeschränkt überwachen können". Apple müsse die Nutzerdaten auf staatliche Anordnung dann herausrücken und habe „wenige bis gar keine juristischen Wege", um derartige Anfragen anzufechten. Apple speichert die für den Zugriff nötigen Schlüssel ebenfalls auf chinesischen Servern. So sei es „praktisch unumgänglich", dass der Konzern gezwungen sein wird, entschlüsselte Daten herauszugeben. Ob Apple dabei in Erwägung ziehe, ob die Übermittlung der Nutzerdaten zu einer Menschenrechtsverletzung führen können, sei noch unklar, so Amnesty – es sei aber wohl nur eine Frage der Zeit, bis sich dies herausstellen werde.

Zwar sei es „bewundernswert", dass sich Apple klar gegen die Integration von Hintertüren in den eigenen Produkten ausgesprochen hat. Dies sei aber letztlich „bedeutungslos", wenn

Strafverfolger die entschlüsselten Daten auch einfach unter Verweis auf ein laufendes Ermittlungsverfahren erhalten können. Amnesty rät ebenso wie Reporter ohne Grenzen chinesischen iCloud-Nutzenden dringend dazu, ihre Landeseinstellungen zu ändern, um den Umzug der Daten auf chinesische Server zu verhindern. Apple sollte chinesische Nutzende dadurch schützen, iCloud standardmäßig nicht zu aktivieren und erst mit „klaren Warnungen auf die Risiken hinzuweisen“. Amnesty erklärte, der iPhone-Hersteller bezeichne Datenschutz als „fundamentales Menschenrecht“. Nun müsse sich zeigen, „ob Apple den Worten auch Taten folgen lässt“.

Der Umzug der iCloud-Daten auf die Server der chinesischen Firma Guizhou on the Cloud Big Data Industrial Development Co. Ltd. (GCBD) fand am 28.02.2018 statt. GCBD gehört der Provinzregierung von Guizhou im Süden Chinas. Als Grund für den Umzug verweist Apple auf „lokale Cybersicherheitsrichtlinien“. Der Kritik könnte sich Apple dadurch entziehen, dass sämtliche iCloud-Daten so verschlüsselt werden, dass diese für Dritte generell nicht zugänglich sind. Derzeit gilt dies nur für einzelne Dienste wie etwa den iCloud-Schlüsselbund. Andere auf iCloud gespeicherte Daten – darunter die umfangreichen iPhone-Backups – kann Apple bislang entschlüsseln (Becker, „Wenn Profit den Datenschutz bedroht“: Amnesty kritisiert Apple, www.heise.de 27.02.2018).

Technik-Nachrichten

Privatkunden-Gentests liefern oft falsche Resultate

Gemäß einer Nachkontrolle einer Stichprobe von 49 kommerziellen Genanalysen, die das Fachjournal „Genetics in Medicine“ veröffentlichte, enthalten 40% der Gentests, die Privatfirmen wie 23andMe direkt an KundInnen verkaufen, falsche positive Befunde, also z. B. Hinweise auf ein Krebsrisiko, das gar nicht besteht. Forschende warnen, dass Laien ohne ärztliche Beratung solche Ergebnisse kaum richtig einschätzen können (Der Spiegel Nr. 14 31.03.2018, 90).

Rechtsprechung

BGH

Verwertung von Dashcam-Aufzeichnungen bei Schadenersatzprozessen zulässig

Der VI. Zivilsenat des Bundesgerichtshofs (BGH) hat mit Urteil vom 15.05.2018 entschieden, dass Dashcam-Aufnahmen als Beweismittel im Unfallhaftpflichtprozess zulässig sein können, selbst wenn die Erfassung nach Datenschutzrecht unzulässig ist (Az. VI ZR 233/17). Dem Kläger ging es in dem Verfahren gegen den Unfallgegner und dessen Haftpflichtversicherung nach einem Verkehrsunfall um Schadensersatz in Höhe von 1.700 €. Die Fahrzeuge der Parteien waren innerorts beim Linksabbiegen auf zwei nebeneinander verlaufenden Linksabbiegespuren seitlich kollidiert. Die Beteiligten streiten darüber, wer schuld war. Die Fahrt vor der Kollision und die Kollision wurden von einer Dashcam aufgezeichnet, die im Fahrzeug des Klägers angebracht war.

Das Amtsgericht hatte dem Kläger unter dem Gesichtspunkt der Betriebsgefahr die Hälfte seines Gesamtschadens zugesprochen. Seine Behauptung, der Beklagte sei beim Abbiegen mit seinem Fahrzeug auf andere Fahrspur geraten, habe er nicht beweisen können. Der Sachverständige erklärte aus technischer Sicht die Schilderungen beider Parteien zum Unfallhergang prinzipiell für möglich. Das Beweisangebot des Klägers zur Verwertung der von seiner Dashcam gefertigten Bildaufnahmen wurde verworfen. Auch auf die Berufung des Klägers erklärte das Landgericht (LG) Magdeburg, die Bildaufzeichnung verstoße gegen datenschutzrechtliche Bestimmungen und unterliege einem Beweisverwertungsverbot. Das LG ließ die Revision zu.

Daraufhin hob der BGH das Berufungsurteil auf und verwies die Sache zur neuen Verhandlung und Entscheidung an das LG. Er kam zum Ergebnis, dass die vorgelegte Videoaufzeichnung nach den geltenden datenschutzrechtlichen Bestimmungen unzulässig sei, da sie nicht auf § 6b Abs. 1 BDSG oder § 28 Abs. 1 BDSG (alt) gestützt werden kann. Jedenfalls eine permanente anlasslose Aufzeichnung des gesamten Geschehens auf und entlang der Fahrstrecke des Klägers sei zur Wahrnehmung seiner Beweissicherungsinteressen nicht erforderlich, da es technisch möglich sei, eine kurze, anlassbezogene Aufzeichnung unmittelbar des Unfallgeschehens zu gestalten, beispielsweise durch ein dauerndes Überschreiben der Aufzeichnungen in kurzen Abständen und Auslösen der dauerhaften Speicherung erst bei Kollision oder starker Verzögerung des Fahrzeuges.

Dennoch sei die vorgelegte Videoaufzeichnung als Beweismittel im Unfallhaftpflichtprozess verwertbar. Die Unzulässigkeit oder Rechtswidrigkeit einer Beweiserhebung führe im Zivilprozess nicht ohne weiteres zu einem Beweisverwertungsverbot. Es bedürfe einer Interessen- und Güterabwägung nach den im Einzelfall gegebenen Umständen. Der Kläger habe ein Interesse an der Durchsetzung seiner zivilrechtlichen Ansprüche und an seinem im Grundgesetz verankerten Anspruch auf rechtliches Gehör in Verbindung mit

dem Interesse an einer funktionierenden Zivilrechtspflege. Dies überwiege gegenüber dem allgemeinen Persönlichkeitsrecht des Beweisgegners in seiner Ausprägung als Recht auf informationelle Selbstbestimmung und ggf. als Recht am eigenen Bild.

Das Geschehen ereignete sich im öffentlichen Straßenraum, in den sich der Beklagte freiwillig begeben habe. Er habe sich durch seine Teilnahme am öffentlichen Straßenverkehr selbst der Wahrnehmung und Beobachtung durch andere Verkehrsteilnehmer ausgesetzt. Es wurden nur Vorgänge auf öffentlichen Straßen aufgezeichnet, die grundsätzlich für jedermann wahrnehmbar sind. Rechnung zu tragen sei auch der häufigen besonderen Beweisnot, die der Schnelligkeit des Verkehrsgeschehens geschuldet ist. Unfallanalytische Gutachten setzen verlässliche Anknüpfungstatsachen voraus, an denen es häufig fehlt.

Der mögliche Eingriff in die allgemeinen Persönlichkeitsrechte anderer (mitgefilmter) VerkehrsteilnehmerInnen führten zu keinem anderen Ergebnis, da deren Schutz durch das Datenschutzrecht Rechnung getragen wird, das aber nicht auf ein Beweisverwertungsverbot abziele. Verstöße gegen die datenschutzrechtlichen Bestimmungen könnten mit hohen Geldbußen geahndet werden. Im Übrigen könne die Aufsichtsbehörde mit Maßnahmen zur Beseitigung von Datenschutzverstößen steuernd eingreifen. Den Beweisinteressen von Unfallgeschädigten werde zudem durch die Regelung des § 142 StGB (Unerlaubtes Entfernen vom Unfallort) ein besonderes Gewicht zugewiesen, wonach ein Unfallbeteiligter die Feststellung seiner Person, seines Fahrzeugs und die Art seiner Beteiligung durch seine Anwesenheit und durch die Angabe, dass er an dem Unfall beteiligt ist, ermöglichen muss. Nach § 34 StVO sind auf Verlangen der eigene Name und die eigene Anschrift anzugeben, der Führerschein und der Fahrzeugschein vorzuweisen sowie Angaben über die Haftpflichtversicherung zu machen.

Mit dem Urteil beendete der BGH einen langwährenden Streit über die Nutzung von Dashcam-Aufnahmen. Volker Broo vom baden-württembergischen Landesbeauftragten für Datenschutz plädierte dafür, nur die jeweils letzten 60 Sekunden festzuhalten und den Rest permanent zu überschreiben. Die Datenschutzbehörden sollten die Autoindustrie auf solche Lösungen verpflichten. Die schleswig-holsteinische Datenschutzbeauftragte Marit Hansen hält die Schaffung einer neuen Rechtsgrundlage für angezeigt, die mit der Automatisierung des Fahren ohnehin notwendig werde (BGH, PM Nr. 88/2018 v.15.05.2018, Verwertbarkeit von Dashcam-Aufnahmen als Beweismittel im Unfallhaftpflichtprozess; Janisch, Dashcam-Videos gelten als Beweise bei Unfällen, SZ 16.05.2018, 1).

OLG Köln

Privat-Router dürfen von Providern auch öffentlich genutzt werden

Unitymedia Nordrhein-Westfalen darf gemäß einem Urteil des Oberlandesgerichts (OLG) Köln die Router, die das Unternehmen den KundInnen stellt, für den Aufbau eines flächendeckenden WLAN-Netzes mittels eines zweiten WLAN-Signals („WifiSpots") nutzen (Az. 6 U 85/17). Eine ausdrückliche Zustimmung der KundInnen („Opt in") ist hierfür nicht erforderlich. Es muss aber für die KundInnen die jederzeitige Möglichkeit bestehen, durch einen Widerspruch aus diesem System auszusteigen („Opt out"). Geklagt hatte die Verbraucherzentrale Nordrhein-Westfalen (VZ). Die VZ vertrat den Standpunkt, dass für die Konfiguration eines zweiten Signals, das ein vom WLAN-Netz der KundIn („1st SSID") unabhängiges WLAN-Netz („2nd SSID") auf dem Router aktiviert, ihre ausdrückliche Zustimmung erforderlich sei. Dieser Argumentation war das Landgericht (LG) Köln gefolgt und hatte der Unterlassungsklage stattgegeben (MMR 2017, 711).

Auf die Berufung von Unitymedia hat das OLG das landgerichtliche Urteil aufgehoben und die Klage der VZ abgewiesen. Die Aufschaltung des zusätzlichen Signals sei keine unzumutbare Belästigung im Sinne von § 7 Abs. 1 UWG. Zwar handele es sich hierbei um eine Belästigung. Der KundIn werde eine geschäftliche Handlung aufgedrängt, um die sie nicht selbst nachgesucht hätte und für deren Vornahme auch deren Entscheidung nicht abgewartet worden sei. Wie bei unbestellter Werbung müssten sich die KundIn mit der Maßnahme von Unitymedia befassen und ihr Aufmerksamkeit zuwenden.

Die Belästigung sei aber bei einer Abwägung zwischen den Interessen des Unternehmens und denen der Kunden nicht unzumutbar. Das Unternehmen habe ein berechtigtes Interesse, sein Dienstleistungsangebot durch Zusatzfunktionen auszuweiten. Außerdem gebe es ein Interesse der anderen KundInnen, Wifi-Hotspots auch außerhalb der Privatwohnung zu nutzen. Demgegenüber sei die Belästigung der KundInnen durch die Aufschaltung des zweiten Signals gering. Ihr Eigentumsrecht sei nicht betroffen, weil die Router unstreitig im Eigentum von Unitymedia stünden. Die Software könne ohne Mitwirkung oder Störungen der KundInnen aufgespielt werden. Anhaltspunkte für eine Sicherheitsgefährdung seien ebenfalls nicht vorgetragen worden. Schließlich bestehe für die KundInnen jederzeit die Möglichkeit, Widerspruch einzulegen, also aus dem von Unitymedia betriebenen System wieder herauszuoptieren („Opt out"). Würde dieser Widerspruchsweg nicht eröffnet, wäre die Belästigung allerdings unzumutbar. Das OLG hat die Revision zum Bundesgerichtshof zugelassen, weil die Frage, inwieweit die Nutzung von im Eigentum des Unternehmers verbleibenden Ressourcen im Haushalt des Kunden zulässig ist, über die Lösung des konkreten Falles hinausreicht (OLG Köln: Unitymedia darf Kunden-Router für Aufbau flächendeckenden WLAN-Netzes nutzen, rsw.beck.de 02.02.2018).

LG Berlin

Facebook zur Rücknahme einer Löschung verpflichtet

Mit Beschluss vom 23.03.2018 verbot das Landgericht (LG) Berlin als erstes Gericht in Deutschland Facebook, einen Nutzerbeitrag zu löschen (Az. 31 O 21/18). Das LG entschied, dass das soziale Netzwerk den Beitrag wieder freischalten muss. In dem Post ging es un-

ter anderem um angebliche „Fake-News“ von „Systemmedien“. Damit stieß erstmals die neue Kommentar-Lösch-Politik der sozialen Netzwerke an Grenzen. Mit dem „Netzwerkdurchsetzungsgesetz“ (NetzDG) werden Internet-Portale wie Facebook, Youtube, Twitter und andere verpflichtet, rechtswidrige Kommentare großteils innerhalb von 24 Stunden zu löschen. KritikerInnen monierten während der Gesetzgebung, dass damit Netzwerke zu Zensurbehörden würden: Sie hätten große Anreize, Nutzerbeiträge zu löschen. Dagegen stünden nur kleine Anreize, die Beiträge stehen zu lassen.

Im konkreten Fall ging es nicht um eine rechtswidrige Äußerung. Der Nutzer aus Berlin hatte einen Zeitungsartikel, in dem es unter anderem um Äußerungen des ungarischen Ministerpräsidenten Viktor Orban zur Aufnahme von Flüchtlingen in Deutschland ging, kommentiert: „Die Deutschen verblöden immer mehr. Kein Wunder, werden sie doch von linken Systemmedien mit Fake-News über ‚Facharbeiter‘, sinkende Arbeitslosenzahlen oder Trump täglich zugemüllt.“ Der Kommentar war von Facebook unter Hinweis auf einen Verstoß gegen die Gemeinschaftsstandards des Online-Netzwerks gelöscht worden und der Nutzer wurde für 30 Tage gesperrt. Den Anwälten des Nutzers zufolge hob Facebook nach einer Abmahnung die Sperre auf, die Löschung aber nicht. Zur Begründung habe es geheißen, eine erneute sorgfältige Überprüfung habe ergeben, „dass die Gemeinschaftsstandards korrekt angewendet worden waren und der Inhalt daher nicht wiederhergestellt werden kann“. Die Gemeinschaftsstandards – also die Hausregeln von Facebook – verbieten unter anderem Hassbotschaften und Gewaltaufrufe. Facebook war in dem Verfügungsverfahren nicht gehört worden und kann Rechtsmittel gegen die Entscheidung einlegen.

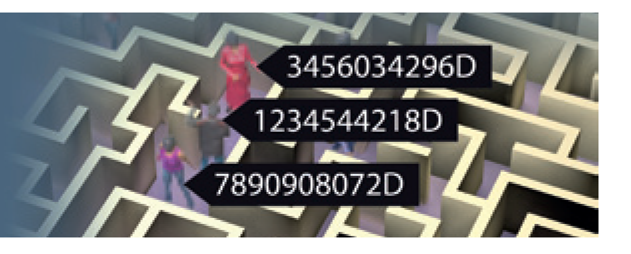
Das LG begründete seinen Beschluss nicht. Die Äußerung des Antragstellers war zweifellos nicht besonders klug; die meisten Deutschen dürften ihr wohl widersprechen. Das Wort „Systemmedien“ stellt ihn zudem in die Tradition des Wortes „Systempresse“, das in den zwanziger Jahren die Nazis geprägt haben. Dennoch hätte der Kommentar, so das LG, nicht gelöscht werden dürfen. Einer der Anwälte des Berliners, Joachim Steinhöfel, kommentierte den Beschluss: „Man mag die Einschätzung des Kommentators teilen oder die Äußerung als polemisch und unsachlich erachten. Wichtig ist nur: Der Kommentar ist von der Meinungsfreiheit gedeckt.“

Das NetzDG, das vom damaligen Justizminister Heiko Maas (SPD) durchgesetzt worden ist, stieß auf massive Kritiker wegen der Gefahr des sogenanntes Overblockings: Aus Angst vor rechtlichen Konsequenzen würden soziale Netzwerke eher zu viele Beiträge als zu wenig löschen und im Zweifel auch legale Inhalte entfernen. Unter dem NetzDG müssen die Betreiber kurze Fristen einhalten. Ihnen drohen hohe Bußgelder, wenn sie strafbare Inhalte stehen lassen. Steinhöfel: „Für das NetzDG ist die Entscheidung des Landgerichts eine Katastrophe“. Es ist allerdings unklar, ob Facebook den konkreten Kommentar auf Grundlage des NetzDG löschte.

Steinhöfel ist kein Unbekannter. Er zieht seit Monaten als Verteidiger der Meinungsfreiheit durch Deutschland, oft eher für Meinungen, die politisch mehr oder weniger weit rechts der Mitte stehen. Zuvor hatte er sich als Rechtsanwalt der Media-Märkte einen Namen gemacht, der immer wieder mittelständische Online-Händler für Formfehler abmahnte und sogar als Werbefigur im Fernsehen auftrat.

Findet einE Nutzende, dass Facebook zu Unrecht ihr Konto gesperrt hat, kann sie im Hilfebereich der Webseite ein Formular ausfüllen: Sie muss ihren Namen sowie E-Mail oder Handynummer angeben und ein Bild des Personalausweises hochladen. Geht es dagegen um das Löschen von Text-Beiträgen, Fotos oder Videos, haben Nutzende kaum Chancen. Eine Facebook-Sprecherin sagt: „Wenn Inhalte gelöscht werden, gibt es keine Einspruchsmöglichkeit. Wir wissen: Das ist frustrierend.“ Im Februar 2018 bemängelte die EU-Kommission, dass Facebook Nutzenden nicht deutlich genug mache, wie sie sich gegen Löschungen wehren könnten. Oft erfährt das Unternehmen erst über Medien, dass fragwürdige Löschungen einzelne Nutzende wütend gemacht haben.

Christian Solmecke, Anwalt für IT- und Medienrecht, erläuterte, dass Nutzende vor Gericht Beiträge wiederherstellen lassen könnten, wenn Facebook seinen Vertrag mit ihnen verletze, was bei der Löschung legaler Kommentare der Fall sei. Das könne auch als Verletzung des Persönlichkeitsrechts gewertet werden. Eventuell sei gar Schadenersatz möglich. In einem Interview hatte Konzernchef Mark Zuckerberg Ende März 2018 darauf hingewiesen, dass Betroffenen sich gerichtlich zur Wehr setzen könnten. Die Chance, Berufung einzulegen, gehöre zu „jedem gut funktionierenden demokratischen System“. Irgendwann solle eine Art unabhängiger Gerichtshof über entsprechende Fälle entscheiden. Aber das ist noch Zukunftsmusik (Facebook darf Nutzer-Beitrag nicht löschen, www.faz.net, 12.04.2018; Einstweilige Verfügung gegen Löschung von Facebook-Kommentar, www.heise.de 12.04.2018; Strathmann, Gericht verbietet Facebook, Kommentar zu löschen, www.sueddeutsche.de 12.04.2018; Brühl, Was tun, wenn Facebook meinen Beitrag löscht? SZ 14./15.04.2018, 10).



Buchbesprechungen



Buchner, Benedikt (Hrsg.)
Der NEUE Datenschutz im Gesundheitswesen
AOK-Verlag Remagen, 1. Aufl. 2018,
ISBN 978-3-553-43100-2, 374 S., 89,90 €

Kurz vor Inkrafttreten der DSGVO veröffentlichte der AOK-Verlag in einer gebundenen Version leicht angepasste Auszüge aus der Loseblattsammlung „Datenschutz im Gesundheitswesen" (DANA 2017, 181). Damit soll insbesondere Datenschutzbeauftragten ein Überblick gegeben werden über die nun geltenden rechtlichen Grundlagen, zum Datenschutzmanagement sowie zu spezifischen Fragen beim Internetauftritt und zur IT-Sicherheit. Das Werk behandelt nicht nur das neue BDSG und das SGB, sondern berücksichtigt auch schon die Novellierung des § 203 StGB, die Outsourcing nicht mehr am Patientengeheimnis scheitern lässt. Anders als die Loseblattsammlung greift die gebundene „Broschüre" den Bereich der Krankenhäuser heraus und berücksichtigt nicht die spezifischen Probleme, die etwa in der Arztpraxis, bei der Pflege oder bei der Rehabilitation auftreten. Auch der technische Teil geht weniger ins Detail. Das Buch setzt keine Vorkenntnisse voraus und ist als Praxisinformation konzipiert. Für eine vertiefte wissenschaftliche Auseinandersetzung mit Themen fehlt es am Detaillierungsgrad und an einem umfangreicheren Nachweis auf weitere Literatur. Dessen ungeachtet liefern ein Stichwortregister und ein Literaturverzeichnis die Möglichkeit zur gezielten Suche und für das Auffinden von weiterführenden Schriften. Also: Trotz des beachtlichen Preises für AnfängerInnen und zum schnellen Nachschlagen eine valide Grundlage.



Kühling, Jürgen/Klar, Manuel/
Sackman, Florian
Datenschutzrecht
4. Aufl. 2018, 355 S., ISBN 978-3-8114-4571-0, 32,99 €

(tw) In der DANA 1/2016 (S. 41 f) wurde schon die Vorauflage freundlich besprochen: Es geht um ein klassisches juristisches Lehrbuch zum Datenschutzrecht, das sich seit der Vorauflage mit der Anwendbarkeit der DSGVO und des neuen BDSG, mit einer Menge neuer Rechtsprechung und einer komplizierter gewordenen Rangbeziehung zwischen Verfassungs- und Europarecht sowie nationalen Bundes- und Landesgesetzen jüngst massiv geändert hat. An die Stelle der bisherigen Autoren Seidel und Sivridis sind dieses Mal neben dem Inhaber des juristischen Lehrstuhls Kühling die (früheren) Mitarbeiter Klar und Sackmann für den Inhalt verantwortlich. Die Konzeption hat sich nicht geändert: Es ist insbesondere geeignet für die juristische Ausbildung, bei der das Datenschutzrecht als exotisches Rechtsgebiet immer noch eher ein Mauerblümchendasein fristet, aber auch für Quereinsteiger, die sich einen Überblick über das Gebiet schaffen wollen, also etwa betriebliche Datenschutzbeauftragte, Compliance-BeraterInnen in Unternehmen, RechtsanwältInnen, RichterInnen oder auch Ministerialbeamte, die erstmals mit dieser Thema etwas umfassender konfrontiert werden und möglicherweise mit dem Datenschutzrecht noch nichts zu tun hatten.

Das Buch ist übersichtlich strukturiert in drei Kapitel: 1. Grundlagen, 2. das Zusammenspiel von DSGVO, BDSG und LDSGen sowie 3. bereichsspezifische Regelungen (besondere Formen der Verarbeitung, öffentliche Sicherheit und Strafverfolgung und Telekommunikationsrecht). Bei den Grundlagen wird das internationale, das europäische und das Verfassungs-Recht sowie deren Entwicklung und Systematik dargestellt. Der zweite Hauptteil ist klassisch aufgebaut und orientiert sich auch an der Struktur der DSGVO. In die Kapitel wird mit 15 Fallbeispielen eingeführt, die am Ende klausurmäßig gelöst werden. Dazwischen wird ein Themenbereich umfassend und zugleich prägnant sowie nachvollziehbar dargestellt. Dabei kann verständlicherweise nicht in die Tiefe gegangen werden. Zwar werden bei den Falllösungen auch unterschiedliche Lösungsmöglichkeiten dargestellt, doch die großen datenschutzrechtlichen Kontroversen werden in dem Lehrbuch nicht ausgetragen. Daher ist das Werk für die WissenschaftlerIn allenfalls als Einstieg geeignet; die technischen Fragestellungen kommen – angesichts der eindeutigen juristischen Ausrichtung – eher zu kurz. Doch wird auf aktuelle Literatur verwiesen, die ja mehr als üppig vorhanden ist, so dass die Tür zum Nachschlagen und Vertiefen geöffnet wird. Einige wenige Schaubilder und Tabellen erhöhen visuell das Verständnis; ein Stichwortverzeichnis ermöglicht thematische Seiteneinstiege.

Auch wenn durchgängig in einem sachlichen Stil verfasst und vielleicht gerade weil keine skandalisierende oder komplizierende Darstellung erfolgt, macht das Buch Lust, sich mit dem komplizierten Rechtsgebiet zu beschäftigen und baut mögliche Einstiegsängste ab.

Insofern ist ihm zu wünschen, dass es insbesondere in der juristischen Studierendenschaft weite Verbreitung findet.



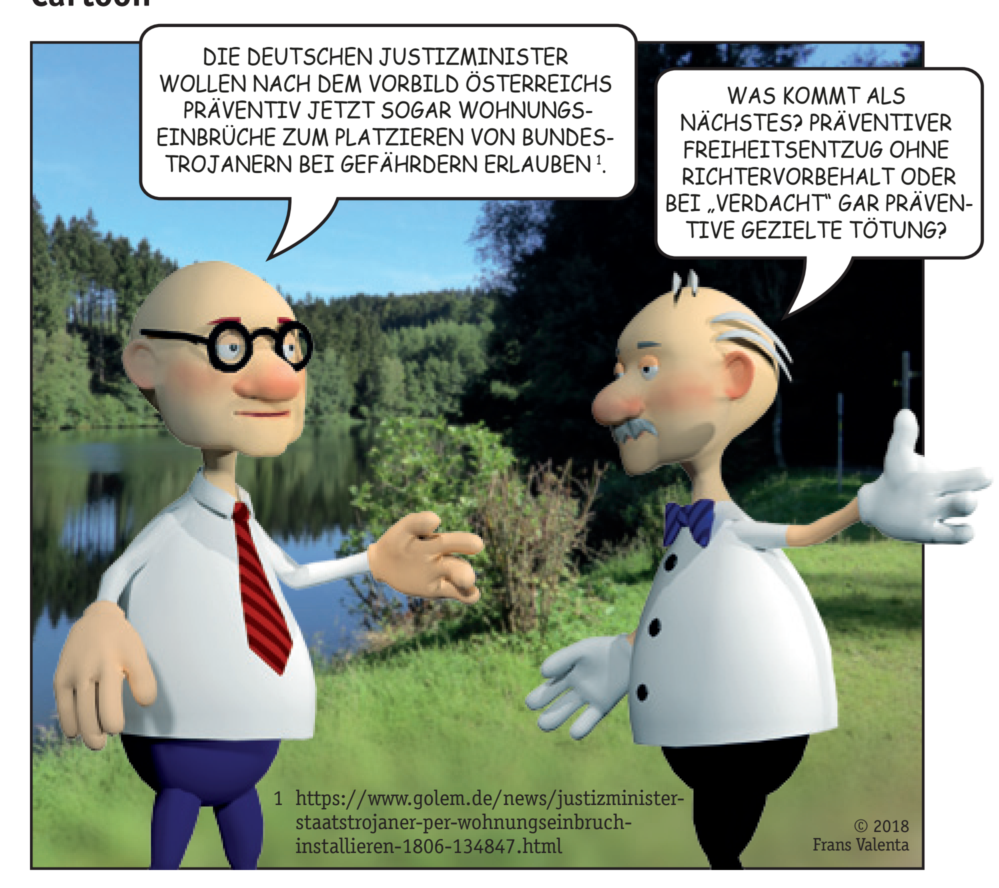
Johannes, Paul C./Weinhold, Robert
Das neue Datenschutzrecht bei Polizei und Justiz - Europäisches Datenschutzrecht und deutsche Datenschutzgesetze -
Nomos Verlag Baden-Baden, 2018, ISBN 978-3-8487-4412-1, 249 S.

(tw) Die Gesetzgebungsorgien im Datenschutz mit den diesen folgenden Auslegungsbedarfen haben kein Ende. Nachdem die europäische Datenschutz-Grundverordnung (DSGVO) und dann das diese umsetzende BDSG bis § 44 umfangreich aber noch lange nicht hinreichend ins Visier der Literatur genommen wurde, geraten nun auch die Randthemen in den Fokus der Datenschutzliteratur. Ein Ergebnis dessen ist das vorliegende Werk der zwei Autoren aus dem wissenschaftlichen Umfeld von Alexander Roßnagel. Der frühe Datenschutzschwerpunkt „Polizei und Justiz" hat sich immer mehr in den privaten Bereich verlagert. Das Polizeidatenschutzrecht hat aber nicht an Relevanz verloren. Das Buch befasst sich mit der europäischen Datenschutz-Richtlinie Justiz-Inneres (im Buch abgekürzt mit JI-RL) und deren nationale Umsetzung in den §§ 45-85 BDSG, 3. Teil.

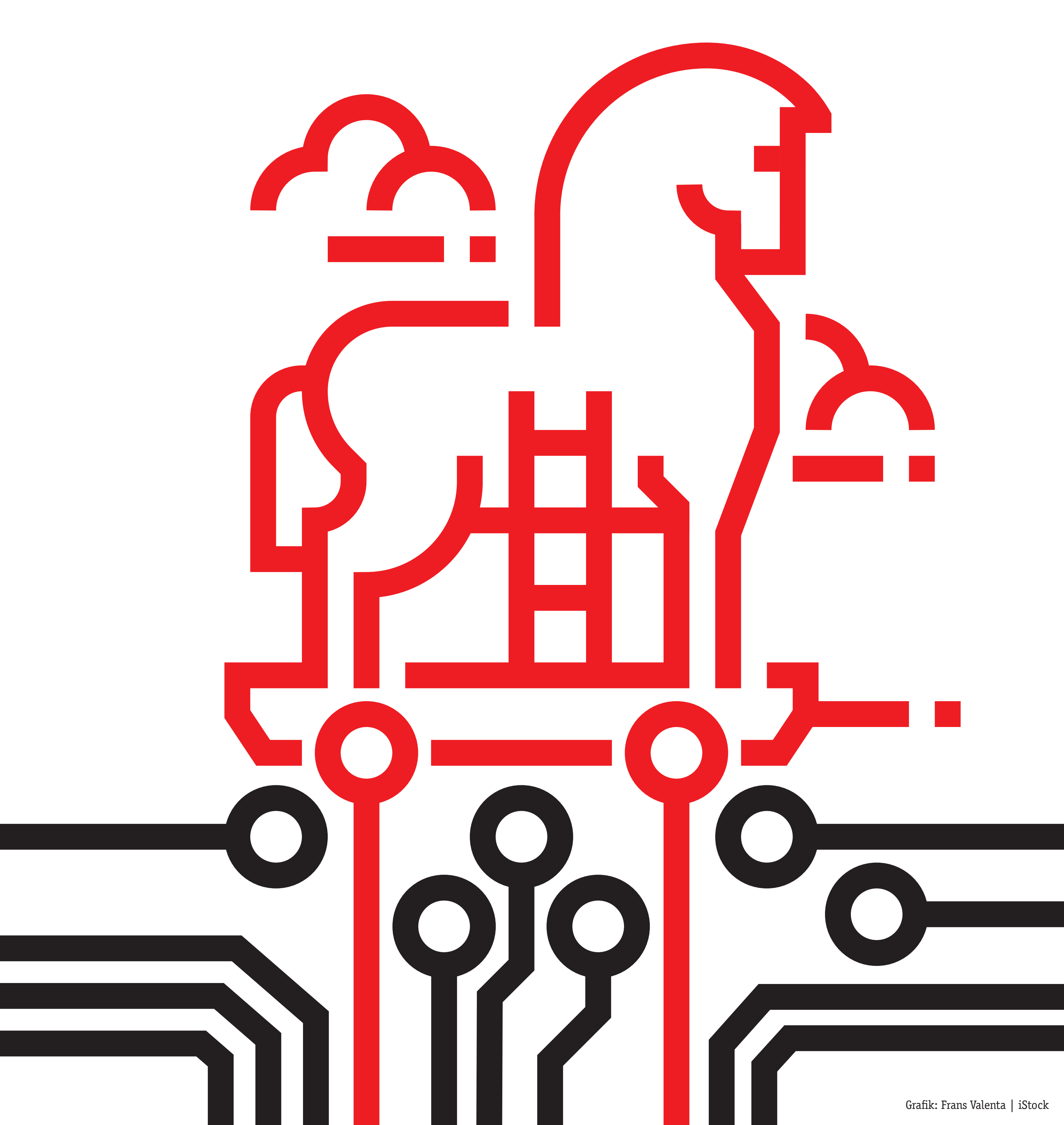
Es handelt sich nicht um eine umfassende Kommentierung des Polizeidatenschutzes. Die Komplexität stieg in diesem Bereich dadurch, dass zusätzlich zu den weiterhin bestehenden Polizeigesetzen bzw. zur Strafprozessordnung die JI-RL gilt, die mit dem hinteren, dritten Teil des BDSG umgesetzt wird. Auch künftig bleibt also der Rückgriff auf die Darstellungen des Polizeirechts nötig. Das Werk beschränkt sich auf die Scharnierfunktion zwischen den Vorgaben der JI-RL und dem in Deutschland vorläufig praktisch unverändert geltenden Polizeirecht mit seinen Datenschutzregelungen.

Dieses Scharnier ist relevant, da es die europäische Teilharmonisierung mit einer Angleichung an die DSGVO bewirkt und weil es zugleich einen allgemeinen Teil für das spezifische für Justiz und Inneres geltende Recht liefert. Die Autoren beschreiben dieses Scharnier in drei Teilen. Im ersten Teil wird ein systematischer Überblick über das Gebiet vorgenommen, wobei die Darstellung weitgehend der Artikel- bzw. Paragraphenfolge der JI-RL bzw. des 3. Teils des BDSG folgt. In einem zweiten Teil ist eine Synopse abgedruckt, die JI- und die dazu passenden BDSG-Regelungen inclusive Erwägungsgründen darstellt. Der dritte Teil gibt eine Kurzübersicht der Nummernzuordnung von JI-RL und BDSG. Das hört sich bürokratisch an; und dies ist es auch. Doch liefert das Buch damit das Material und den Schlüssel zur Europäisierung des Polizeirechts. Ohne dabei zu sehr in die Tiefe zu gehen, gibt es die nötigen Hinweise, um praktisch mit dem dritten Teil des BDSG, also den JI-Regeln, arbeiten zu können. Dabei wird die vorhandene Literatur ausgewertet, und teils auch über Hinterfragungen so manche Umsetzung in ein kritisches Licht gesetzt. Dabei verfolgen die Autoren eine grundrechtsfreundliche Sichtweise, die in nüchterner Weise vorgetragen wird, etwa die Kritik an den fehlenden Abhilfebefugnissen der Datenschutzaufsicht. Sowohl die Art der Texterschließung wie auch die Präzision der Darstellung und die weiterführenden Hinweise erfüllen nicht nur die Bedürfnisse von Praktikern, sondern auch von Wissenschaftlern. Zugleich kann das Werk als Referenz genutzt werden, wenn nun die JI-RL auch im Landesrecht umsetzt wird, was gemäß dem Bundesvorbild zumeist in einem Extra-Teil der Landesdatenschutzgesetze erfolgt.

Cartoon



Wie wendet man eigentlich das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ bei **Bundestrojanern** an?



Grafik: Frans Valenta | iStock